ETAG

European Technology Assessment Group
ITAS · DBT · viWTA · POST · Rathenau

RFID and Identity Management in Everyday Life

CASE STUDIES ON THE FRONTLINE OF DEVELOPMENTS TOWARDS AMBIENT INTELLIGENCE

Deliverable No.2

of the project
"RFID & Identity Management"
commissioned by STOA and carried out by ETAG

Contract No.: IP/A/STOA/SC/2005-182

Ref.: Framework Contract No. IP/A/STOA/FWC/2005-28

October 2006

Report prepared by Christian van't Hof and Jessica Cornelissen,
The Rathenau Institute, The Netherlands

European Technology Assessment Group
- Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe
- Danish Board of Technology (DBT), Copenhagen
- Flemish Institute for Science and Technology Assessment (viWTA), Brussels
- Parliamentary Office of Science and Technology (POST), London
- Rathenau Institute, The Hague

Contact:
Dr Leonhard Hennen (Co-ordinator)
Institut für Technikfolgenabschätzung und Systemanalyse
Forschungszentrum Karlsruhe
c/o Helmholtz-Gemeinschaft
Ahrstr. 45
D-53175 Bonn

Preface

This is the second of three deliverables within the ETAG project RFID & Identity Management. The purpose of this deliverable is to provide insight into real life experiences with RFID and counter both doomsday scenarios and over-optimistic future predictions of this new application. We performed 24 case studies to describe the use of RFID technology in events which occur on a daily basis: taking public transport, driving a car, going to work, shopping, having fun, crossing borders and receiving treatment. Our accounts demonstrate how RFID is currently playing a role in the lives of Europeans – sometimes for the better, sometimes for worse.

The project is carried out for the European Parliament by the Dutch Rathenau Institute as part of the STOA consortium. The case studies are performed by a team of researcher at the Rathenau Institute: Christian van 't Hof, Jessica Cornelissen, Sil Wijma, Eefje Vromans and Elisabetta El-Karymi. This report is written by Christian van 't Hof and Jessica Cornelissen and reviewed by Chandrika Nath from POST, UK. In the next and final deliverable of this project, the empirical findings have been taken as input for two creative sessions in which we developed scenarios on different settings in which RFID is used.

Contents

Introduction: when RFID becomes a personal ID

RFID stands for Radio Frequency Identification and refers to information systems consisting of RFID chips exchanging data with an RFID-reader at radio frequencies. RFID is currently used to identify persons (passports, employee ID cards/tokens, pay systems), objects (cargo, retail, devices) and animals (livestock, pets). In this research we focus on people. Although the largest volume of RFID is in logistics, where the smart tags are used to identify cargo, it currently enters the public domain on a massive scale. This chapter describes how RFID works, how it is used to track people and what it means to manage ones identity in smart environments.

RFID systems tracking movements

An RFID chip contains a small chip and an antenna to communicate on radio frequency. The chip can be active (giving a signal powered by a battery) or passive (powered through induction in its antenna by the signal from the RFID-reader). The data on the chip can be fixed or rewritable. When an RFID-chip is scanned, it provides the information needed on that location. It can also just deliver a code which serves as a key to unlock information on the identity of the chip from a central database. The combination of an unique identity and the place and time the identity is displayed can serve to track movements through an RFID system. Specific persons can be identified once the database can link the identity number of the chip to the person carrying it, as is the case with ID cards. Once the identity is confirmed, the system can respond by opening a door, providing information, performing a transaction, or any other kinds of services. Meanwhile, both the service, as well as the combination of ID, place and time is registered. This is described in the figure below.

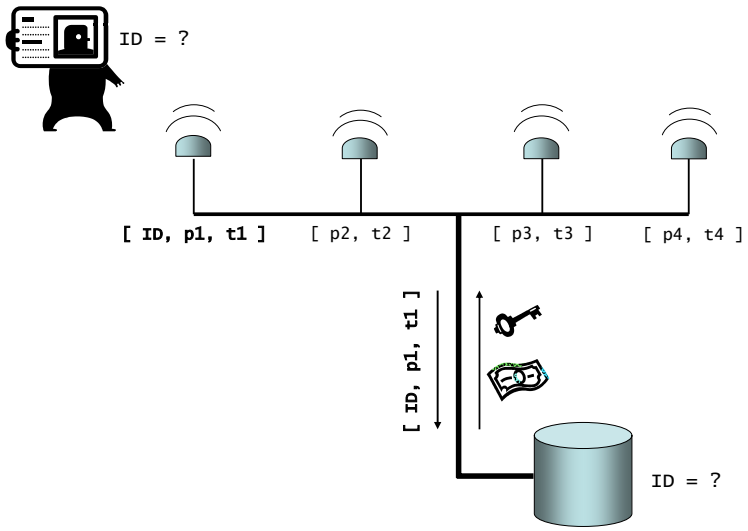

Figure 1: tracking movements within an RFID system

This information on people could be valuable and there is a risk that "function creep" could occur: although a system may be built for a specified function (such as securing access), once it is in place many opportunities open up for which it was not originally intended. Supermarkets are among the best known cases. Tagged groceries in combination with RFID customer loyalty cards for example could tempt marketing departments to direct marketing actions based on customer behaviour. This has led privacy watch groups such as FoeBud (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs) in Germany and CASPIAN (Consumers Against Supermarket Privacy invasion and Numbering) in the US the organise public protests against the use of RFID.

Legislation

In terms of legislation, such cases are covered by EC Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This directive builds upon the OECD Privacy Guidelines, which form the basis for many national laws on privacy. These laws state for example that people are entitled to know what kind of information is gathered about them, for a purpose specified in advance. In that sense, a function creep is illegal once the user has not been informed in advance. Still, not everyone is aware of the guidelines and they are hard to enforce given the rapid increase in RFID systems. Moreover, in some cases one can debate whether the RFID system is registering *personal* information when people are tracked anonymously, for instance through a tagged basked or shopping car. At the time of writing, the European Commission is reviewing the Directives on the basis of an extensive public hearing on RFID. Results can be expected in October 2006.

Managing identity in smart environments

The public image of RFID is currently caught in the middle of two opposing camps. On one side, there are pressure groups, journalists and members of the public predicting a dark future with a the Big Brother scenario unfolding. Their key words are: spy chips, privacy and surveillance. On the other side, there are the business promoters painting colourful pictures of a bright future in which everything is smart, safe and automated. Their keywords: solutions, innovation, efficiency, return on investment and usability. Still, the technology in itself is neither evil nor good and whether the future will be dark or bright will depend on how users and owners of RFID systems will use it. In order to avoid taking one side of the debate, we introduce a more neutral and dynamic concept with regard to the storing and use of personal data : Identity Management.

Identity Management is an activity involving two actors: the owner/maintainer of the RFID environment and the user of this environment. From the maintainers perspective Identity Management can involve safeguarding a specific person (employee, traveller, citizen) logging into the system actually is who he states to be. Additionally, once the person is identified, all sorts of identity aspects can be attributed to this person: “this employee is allowed here and currently at work” or “this customer has paid and is a frequent visitor”. This activity also takes place from the side of the user, but then from their perspective: “I am allowed here” or “I am a loyal customer”. The identity being managed by both maintainer and user can be similar, but this is not always the case. Users could want to define their identity just as “having access” or “having paid”, while the maintainer of the environment might attributes additional identity features to the person, either overtly or covertly. Sometimes a third party also enters the activity, such as direct marketing organisations looking for “a potential customer for additional services” or police searching “potential criminals” on the basis of travel profiles.

In summary, we define Identity Management as how a person, interacting with an information system, defines what is known and not known about him/her to others using the system and how this relates to the information known or not known to the persons maintaining the system. In others words: identity is mutually defined instead of one-way. In some cases, identification through RFID has led to controversies, in which the identified tries to take control back from the identifier. In other cases, both owners and users of RFID environments agree upon the mutual benefits. This activity differs from one system to another, depending on the technology used and the people using the system, i.e. the relationship between the owner of the RFID system and the person carrying the RFID-chips.

Aim and methodology

This research aims to provide insight into how users and owners/maintainers of different environments manage identity. Identity Management is understood as how a person, interacting with an information system, defines what is known and not known about him/her to the system and how this relates to how this is defined by the owner of the system.

Research questions

In order to reach this aim, the following research questions are formulated:

- In what kinds of settings are RFID systems used to identify people?
- What purposes do the RFID systems serve?
- What kind of information is stored on the chip and database of the RFID system?
- How do users and owners of the system, consciously or unconsciously, influence what kind of personal information is known?
- What are the tradeoffs of providing more or less personal information?
- What choices are available to the users and owners of the RFID-systems in interacting with the system?

Methodology

Being still relatively invisible in the public debate, RFID is difficult to investigate through quantitative methods. A survey by Cap Gemini for example 'RFID and Consumers' (2005), showed very few European citizens even know what RFID is, let alone have formed an opinion on it. Only 20% had ever heard of RFID and the respondents who could state an opinion needed much additional technical explanation. As the awareness is still low and the net sample of actual experience will be too small, surveys can merely scratch the surface of how users actually deal with smart environments. The case study method therefore applies more to this issue, as it can both provide a broad view of the situation as well as a more in-depth analysis of what actually happens once people use RFID systems.

A case study is defined as a qualitative description and analysis of an event, specified in time and place, with specified actors (organisations or individuals). In theory, a single case study can be the base of empirically based claims. In order to analyse the use of RFID in different contexts, we need a broader empirical base by performing a number of case studies. To strike a balance between both empirical depth and broadness, we use a funnel approach, which starts with a broad variety of less-detailed case studies to survey the area and funnel down to a small number of cases to be investigated more thoroughly. In our research, we distinguished four levels:

Level 0 case: Description of function of a specific RFID application (e.g. access, payments), where and when it is used by who in what kind of setting (e.g. public transport, leisure).

Level 1 case: Level 0 + desk research (reports, websites, newspapers, etc.) to describe users and maintainers and possible Identity Management issues.

Level 2 case: Level 1 + additional inquiry through e-mail or phone contact.

Level 3 case: Level 2 + site visit to observe users and hold interviews with people involved.

We started with 140 level 0 cases throughout Europe, gathered through internet searches, from experts, books, journals and newspaper articles. This pool of cases also provided us an overview of settings in which RFID is actually implemented and enabled us to draw a sample of cases for each setting. We then selected 24 cases for level 1 research. The selection criteria were:

- Human identification: the RFID application must be used identify people, either as personal identification or anonymous as "visitor", "user", etc.
- Geographical spread: cases must come from different European countries. (If relevant, an US or Asian case can be taken in consideration for comparison, but not for level 2 or 3.)
- Neutrality: many reports on RFID serve as showcases for business purposes, e.g. a business case or best practice. These case descriptions need to be avoided.
- Multiple sources: in order to balance different perspectives on the story, a case must be studied from multiple sources, e.g. a journal article, an organisational website, etc.
- Traceability: the information on the case must have a recognisable source, to enable checks afterwards.
- Maturity: the case must reach beyond the planning phase, be a pilot or a fully established RFID application.

Eight cases that proved to be most interesting were taken forward through e-mail contact, on line newsgroups and phone calls (level 2). Five of them resulted in an actual site visits (Level 3), at which we observed users of the system and interviewed people involved: a database maintainer, marketing manager or security officer and users we occasionally met. The selected 24 case studies are documented in the appendix in a standard format, containing the following items: setting, technology, actors involved, Identity Management issue, case story and sources. These 24 cases are the basis for the next chapter where we describe the role RFID plays in an ordinary day in the lives of Europeans. For the sake of readability, the references to the source material and technical details of the applications are only described in the appendix.

Results: RFID and Identity Management in everyday life

This could be any day in an ordinary life: a person going to work by public transport, taking a car to go shopping and having fun afterwards. In every setting, RFID displays an identity of this person to gain access to services. In return the maintainer of the RFID environment receives valuable information on this person. First of all on access: is this person allowed here? Once the systems are implemented and the databases start running, they provide much interesting information, sometimes even more than anticipated. Profiles start to emerge on movements, spending, productivity, preferences, habits and so forth. These case studies demonstrate innovation takes place in practice, sometimes for better and sometimes for worse.

Taking public transport: payments and profiles

Many public transport organisations in Europe are currently replacing paper based tickets in plastic public transport cards with RFID chip. These passive and partly rewritable chips are being read on entering a bus, metro, train or ferry. Most cards work as a debit card: money needs to be put on it before travelling, either by putting cash into a machine or a bank transaction. Some cards are more like credit cards: the costs of travelling are purchased by the company after the trip took place. Debit cards can therefore, in principle, be anonymous as the traveller has already paid, while for credit cards full personal details are needed in order to secure payments are fulfilled.

As long as the RFID system merely functions as a payment system, Identity Management is basically a matter of distinguishing between people who have paid or not, in some cases differentiating between one-off tickets, some forms of discount or seasonal tickets. For the user, it's just like any other payment system. For the maintainer however, many opportunities open up to monitor travelling behaviour. With paper tickets, identities connected to it were cut off at the exit. With RFID, the link remains through the unique code which is scanned on every entry or exit. Sometimes this identity can be anonymous, for example "traveller X entering Bus 1 at 10.05, taking Bus 2 at 11.40." This provides information for building profiles, such as: "people going from A to B, also travel frequently between C and D". This can be valuable information for the marketing or the logistics department. In the following cases, cards are also linked to a specific name, address and bank account – opening up many opportunities for direct marketing or crime investigation.

Remarkable enough, we found relatively few cases in which this use of RFID triggered any debate. One such example is the **VRR/VRS Card** [case #123] in North-Rhine-Westphalia, Germany. The German Verkehrsverbund Rhein-Ruhr (VRR) and Verkehrsverbund Rhein-Sieg (VRS), was in 2003 Europe's biggest case in implementing smart cards in trains and busses. The cooperation involved 54 different transport operators covering the whole region of North-Rhine-Westphalia, with a total population of 10.6 million inhabitants and handling 1.1 billion passengers per year. The main advantage of the e-Tickets is that travellers don't have to buy a ticket anymore. A card reader which is placed in the bus or train registers where the cardholder gets on and off. At the end of the month the costumer gets the bill.

Privacy watch group Foebud (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs) did warn on its website the travel data could be used to monitor movements of people and make extensive use of personal data. Still, we found very few accounts of people or organisations who claim VRR/VRS actually uses the cards for other than making transactions. VRS/VRS also explicitly claims only the relevant data necessary for the validity of the card are stored on the chip: name, validity-date and "zone-validity". No travel details or more personal data are stored. Customers can even choose if they want to pay with a personalised credit card or an anonymous debit card.

In the case of **SIpass** [case #84] in Italy the maintainer of the RFID environment goes a little step further in using personal data from travellers. This RFID card was introduced during the Olympics of 2006 to pay, among other, in public transport. Mr. Aliverti, Sales Director at Gruppo Torinese Trasporti stated: "This new system will not only help us to combat fraud but also enable us to collect data so that we can offer customized fares and value added services to travellers". When we acquired the application form, we could read the following statement:

> "Personal data is collected solely for employment related purposes or for use in connection with other such matters. Personal data shall be disclosed or made accessible to third parties exclusively for the aforementioned purposes. TURISMO TORINO hereby guarantees that anyone may request access to their personal data at any moment in order to up-date, change or supplement such data, and may oppose such data being used for the purposes given above."

This formulation provides a certain level of Identity Management by gaining control over the use of their personal information, but, other than with the VRR/VRS Card, they have to do something for it. Still, in our research we did not encounter any negative responses to this use of data. Either the Italians agree their identity is managed as such, or they are just not aware of it. Meanwhile, London got its **Oyster Card** [case #61], which demonstrated another Identity Management by a third party: police identifying criminals through travel profiles.

This RFID card was introduced in August 2004 and is currently used by 5 million people. The card serves to pay on busses, the subway and some trains. On purchasing the card, one has to fill in full personal details: name, address, phone number and e-mail address. This is apparently to fulfil the transaction in order to obtain the card. But it could also be used to track specific persons through the public transport system, as was claimed by The Guardian in January 2006. According to this British newspaper the police in very interested in using the journey data that is stored from travellers who use the Oyster card: a total of 61 requests were fulfilled in January 2006 alone. In a response, a spokesperson form Transport For London stated:

> "Transport for London complies fully with the Data Protection Act. Information on individual travel is kept for a maximum of eight weeks and is only used for customer service purposes, to check charges for particular journeys or for refund inquiries. […] A very few authorised individuals can access this data and there is no bulk disclosure of personal data to third parties for any commercial purposes. There is no bulk disclosure of personal data to any law enforcement agency. If information is disclosed, it is always done so in accordance with the Data Protection Act after a case-by-case evaluation."

Indeed, data protection laws prevent personal data being hand over to anyone without the consent of the person involved, with exemption for police investigation. Still, being seen as a potential criminal is not the kind of identity the user of this environment was hoping to manage. As demonstrated before, this easily triggers Big Brother Scenarios, perhaps even beyond the wished of the maintainer of this environment.

According to a weblog on the Oystercard, yet another involvement of third parties may trigger Identity Management issues: conspicuous spouses using their partners' card to track their movements. The travel data appears to be accessible through machines at stations and via a website, using only the registration number of the card. But whether this actually occurs on a large scale remains to be seen. All in all, these RFID systems do provide much more possibilities than just payment. Still, while they are employed on a large scale throughout Europe, few controversies arose. One case in the Netherlands however did result in a large national debate on Identity Management: the Dutch **OV-Chipkaart** [case #56]. This application is expected to be Europe's first nation-wide, multi modal public transport card. With this card travellers will be able to pay at busses, trains, subways, trams and

ferries throughout the whole Netherlands. But already during its first implementation phase in 2005 and 2006, Identity Management issues triggered a national debate.

Owner and maintainer of this RFID environment is Trans Link Systems (TLS), a consortium of the five largest public transport companies in the Netherlands, representing 80% of the Dutch market. Travellers are represented by a whole host of organisations, such as two travellers' interests groups (Locov and Rover), the Dutch Data Protection Authority (College Bescherming Persoonsgegevens), a consumer organisation (Consumentenbond) and a privacy watchgroup (Bits of Freedom). Even the Dutch Parliament got involved and discussed the issues at more than 20 meetings. The Dutch minister of Transport took position as mediator between the maintainer of this RFID setting and organisations protecting the interests of its users. Because of the scale of both the system as well as the controversy, we analysed this case quite thoroughly, using governmental documents, user evaluations from Translink, publications from privacy organisations and pressure groups, newspaper articles and on line newsgroups. We got our own OV-chipkaart too, to see how the system works and talk to other travellers.

The OV-chipkaart contains a passive rewritable RFID chip, which contains a unique number and a rewritable section to store information on travel time and uploaded value. Users can opt for an anonymous card or a personalised card. In case of a discount or season ticket a personalised card is obligatory. Buses and trams have readers placed at the doors, where people check in and out. Now and then a security officer with a hand-held reader goes through the bus or tram to check on fare dodging. At the train and subway stations travellers check in at the platform, holding their card near a reader in order to open a gate. At the start of the project, the total cost were estimated at to be €.1.5 billion of which a small part would also be paid by local and national governments. A first large pilot was held in 2005 in the city of Rotterdam and the region South West. About 30.000 test travellers started using the card in the metro, bus and one rail track from the city to the beach. A second pilot is currently held in Amsterdam.

In order to get an OV-chipkaart ourselves we needed to fill in an application form requesting many personal details: name, address, bank account, signature and a copy of our passport. This is quite surprising, as the card is a debit system and not a credit system. Money can be put on the card through machines placed at the stations and we did not see why identification was necessary. According to Translink Systems anonymous card should also be available in time, but these were not offered yet. Another OV-chipkaart was sent automatically to us by the Dutch Railways, replacing a discount card we already possessed and for which we already provided personal data. The accompanying letter proclaimed we were now "prepared for a new way of travelling". It also stated that, once we waved our card the first time at the reader, this act would be interpreted as an opt in for the user agreement. For details on this agreement we were referred to a website. Although this action can be interpreted as service in order to make the transition more smooth, it is a subtle way to get a personalised card more accepted than the anonymous card.

On the subway, the OV-Chipkaart worked quite well. When holding our card near the Translink sign, the reader bleeped, displayed the current value of the card, stated we had checked in and wished us a pleasant journey. We did however not have to use the card to open the gates. These were left open for people still using the paper-based tickets. On the buses however many problems occurred. Sometimes we could not check in. The readers just gave a mysterious code: 707. Most of the bus drivers could not handle the malfunction, made some jokes about them and offered us a free ride. On other occasions, the readers did not sufficiently check us out, resulting in a payment for as far the bus would go. One of our researchers made 40 trips and accounted more than half of the transactions failed. A bus driver, helping her out on many of these events, called her one night at home to inquire if everything was sorted out with the card. This account demonstrates the link between the card and the personal information in the database has not been sufficiently secured yet. Finally, at one occasion we were checked for fare dodging by a controller with a hand held reader. We then found out the data on the card also contain our date of birth – yet another bit of identity being managed by the maintainer without our consent.

According to an evaluation of the Rotterdam pilot many other people had difficulties with checking in and out of the buses. About 25% of the respondents claimed there are too many problems with malfunctioning of the system. But what this evaluation did not account for, was how the users felt about what was being done with the data they generated. It took the Dutch Data Protection Authority to bring the issue out in the open. Many national newspapers followed suit and a controversy was born. It revolved around two issues related to tracking people throughout the system: price differentiation and direct marketing. Moreover, central in these issues is the degree of free choice users have within the system to manage their identity.

From the start of the project, the Dutch Railways (NS) have been open about the fact they favour personalised cards and will use the data generated by travellers for marketing purposes, without specifying what kind of marketing. This led the Dutch Data Protection Authority in February 2006 to warn the NS and other public transport corporations that their storage and use of travel information was not always legitimate. The CBP stated that, according to the Dutch law on protecting personal data, the aggregation of data has to be limited to the necessary data – in this case data for administering payments and not for marketing - and data can only be used once the person involved has agreed explicitly. In response the Dutch Railways said they interpret this law differently and claim they can store and use the data as they deem necessary and travellers still have a choice to travel anonymously. Still, personalised cards turn out to be temporarily cheaper than anonymous cards. Also, no *explicit* user consent is sought to the data policy of the NS - as we encountered with our discount card, simply using the system is seen as acceptance of the data policy. Finally, for discount cards and season ticket personal data is obligatory, as it is needed to automated billing.

A second issue concerns price differentiation. According to calculations of Locov, a consumer organisation of public transport users, the RFID system will be used to enable unfair price differentiation. Costs of travelling in rush hours for example will rise with 10% while travelling outside these hours will cost 20% less. They consider this to be unreasonable, because most travellers have no choice but to travel during rush hours. Another price differentiation they consider unacceptable is the difference in price depending on whether the user specifies his destination before travelling. Travellers entering the public transport can specify beforehand were they are going, or just check in and out. The price of the latter option is 10 to 100 percent higher, depending on the trip. Locov expects most travellers will specify their journey beforehand thus limiting the usability of the card.

Reactions on the internet show that many people currently have doubts on the OV-chipkaart system. On the forum Tweakers.net for example, some test travellers praise the system because it is easy to use as you just have to wave your card before a reader. But many others are afraid of the idea that more and more information about themselves and their whereabouts is registered. Some fear the police soon will get access to all travel data, or data will be used for all sorts of commercial purposes such as advertisements. Others worry about the security of the travel data, especially when this data will be accessible over the internet. Some especially criticise the lack of choice: when using the public transport regularly - and therefore use a discount card or a subscription - they cannot travel anonymously. Finally there are people worried that the OV-kaart system is to complex for many people, especially elderly. Because of these concern people are already searching for ways to undermine the system; for example by exchanging cards with each other and thereby confusing the Identity Management schemes of the maintainer of this environment.

The Netherlands once had the ambition to be the first European country with a nation wide, multi-modal RFID public transport system in 2007. One card should give travellers access to buses, trams, metros, trains and ferries throughout the whole country. But opinions on Identity Management still differ to a large extent, hampering a system which once promised efficiency and usability. Currently, the debate in parliament has stopped due to elections, but according to the minister of transport, the Dutch Railways can move forward with implementing the system. Nevertheless, the national roll out is now postponed until 2009.

Going to work: access and presence

The working environment is perhaps a setting where we can see some of the oldest applications of RFID for Identity Management. In the last decade many offices have switched from the normal iron keys or magnetic cards to RFID. Surprisingly very few studies exist of RFID use in this area. One exception is a study from the RAND corporation on five large offices in the US. Their accounts demonstrated that none of them used RFID merely as a key. Although the systems were put into place by the security departments and managed as such, other departments soon took interest in the information gathered, such as Human Resources, the legal department and line management. [Balkovich et al, 2005: p.12] Many functions were added, such as time registration, as we will see in our European cases too.

At the **NWO office** [case #96] in The Hague, the Netherlands people are still learning that the small plastic token they hold is not just a key, although it appears to be at first sight. On entering their office, they go through several doors which are secured with an electronic lock: from the underground car park, to the elevators and on each floor. Readers are placed next to the door handle. The RFID tag can be read when it is held less then a centimetre from the reader. The unique code is sent to the database, which checks whether the token can provide access. If it does, the door opens, if it does not, the door remains closed and the system operator receives a signal on his screen. At every reading the following information is stored in a central database for an unlimited time: door, department, time of entry and name of employee.

This key function is extended by the possibility of differentiating levels of access. Token holders can be given access just on the route to their place of work from 7.30 up until 19.00 and some of the general facilities such as the canteen. Access can be extended at the central database: allowing personnel to also visit offices of other organisations in the building, or get access beyond the time limits. We discovered a lively trade evolved around this extension, especially between different organisations residing in the building. In our interviews, the system administrator appeared quit strict about the rules: only permanent staff can get the key, with fixed level of access. However, the system operator, who has access to the database appeared to be more flexible, demonstrating Identity Management is not quite fixed, but negotiable.

Many people succeeded in obtaining additional tokens for temporary staff, although this is not allowed. Also, one head of facilities convinced the system operator to bring her own access level up to a higher grade and that of others down, providing her with access to all other offices, while she got all other personnel from other offices rejected - even the service people who needed to access the office for maintenance. Another employee also turned out to have extended access: this was revealed when staff were having a celebratory drink down the hall one day and they discovered they could not enter their offices again because it was past 19.00. To everyone's surprise this employee's token opened all doors while others were locked out, even the director of the organisation.

In our time in the office, we asked several people on what they thought of the system. Almost all of them were surprised to find out their check in time was registered and assumed the system to be nothing more than an access system. The System Operator also told us an interesting story on one employee who discovered that the token is more than just a key. His colleagues and supervisor saw him leaving quite early every day, while he claimed he also started very early when others were not there. The supervisor then went to the system operator and requested a table of check-in times of this employee. The data were in fact showing the staff member did not always start as early as he claimed to. The system administrator however refutes this story, reclaiming the primary function of the system: access, not time registration. Still, a database administering the whereabouts of all staff, may prove to be too valuable to be merely used as an access system.

This case study can be seen as a very basic example of RFID and Identity Management in offices. We now go to the offices which do overtly use RFID for tracking personnel real-time. In order to do that, some practical, but essential adjustments must be made on the system. Most passive RFID access devices are mainly used to enter, but not to exit buildings. Serving its function as a key, the person only has to identify at entrance, while a push button at the other side provides an easy exit. Also, once one personnel member has opened the door, several colleagues can come along leaving no trace in the database. A football stadium kind of turnstile could be a solution, but may obstruct the movement of personnel too much and be less suitable to the office culture. One solution could be stepping up from passive to active RFIDs, tracking movements real-time, anywhere on the premises, as we can see in the cases below.

Mol-Logistics [case #128] is an international company specialising in logistics and has considerable experience of using RFID for cargo. The technology is now extended to monitor personnel movements too. Their location in Tilburg is divided into zones by a number of strategically placed RFID readers, both at the truck area as well as the offices. Each truck driver and office staff member carries an active RFID tag which broadcasts a unique signal every 1.5 seconds. The database thus provides a real time image of who is present in which zone, managing the identity of all people inside the premises based on time, place and access levels. First of all, the active RFID tag serves as a key to open the fence, providing access to drivers and as a hands free door opener at the offices. Secondly, it also serves to deny access, for example for visiting drivers who receive active tags too. As long as they remain in the docking area nothing happens. Once the visitor moves into a restricted area, for example the warehouse, an alarm is triggered. Thirdly, at the offices, the tag functions as a punch card, registering time-in and time-out as personnel enter and leave the office. Finally in case of an emergency, security personnel can immediate spot whether there are still people in the danger zone.

It is reasonable to assume that the logistics sector might readily adopt RFID as they already have broad experience with it. But what will happen if this system is used in an office environment? **Alcatel** [case #126], the international telecom company, tried this. Although the system was initially perceived as a “Big Brother tactic” it turned out to be in favour of the staff when the Working Council addressed the issue of overwork.

In the beginning of 2005 the Alcatel office in Rijswijk, the Netherlands shifted from magnetic card access to active (battery powered) RFID access. All employees received a thick card (100, 50, 5 mm), with a picture on it of themselves, to be carried visibly at all times. An active RFID chip inside the card broadcasts a signal every 1.5 seconds. Readers are placed at all doors and throughout the halls. The system as a whole registers the whereabouts of all the tags in the building in real time. Guests at the office also receive an active tag, of which the identity is linked to the person receiving the guest. Valuable devices such as lap tops and beamers are also tagged with active RFID. This serves several functions: automatic hands-free access, evacuation management, time registration and theft prevention. This is what the system is supposed to do. But according to several people we interviewed at the office, some remarkable things happened.

First, the automated access. On arrival, employees go through three access points: the parking lot (if they come by car), entrance to the building and the staircase or elevator. With active RFIDs, the users should not have to hold their cards near a reader, but just wave it in its direction or not at all. Still, the communication between tag and reader does not always work properly. The reader at the entrance of the parking lot appears to have its moods, presumably depending on the weather. Some readers on one floor appeared to register people moving on another. This was just a matter of adjustment. A problem remaining is that the exit reader does not always register exit, presumably because several people move through at the same time. Also, as many other offices, this building has several exits clustered together, causing a single approaching employee to open the elevator, hall door and fire escape at the same time - the latter setting off an alarm.

Second, the evacuation management. Every now and then, the Alcatel office holds an evacuation drill. Facility Manager Hans van der Kooij then sets off the alarm and the staff are expected to leave the

building. The system then provides a table of all active RFID tags left in the building, presumably of employees in hazard. At their first drill with the new system, Van der Kooij came out last, disappointed, holding four tags with no employees attached. In case of a real fire, this may have caused a fireman to risk his life, searching through the smoke for injured workers, only to find a tag left on the desk.

Third, time registration. The database registers the time of entry and exit of all employees. The net time spent in the office is presented in a time registration sheet to the employee, who then justifies hours spent on projects. This system may appear like a punch card system but it actually isn't. The simple reason for this is that less than 25% of staff perform their work only in the office. The rest of them are continuously on the move for their clients. Also some people live quite distant from the office and are allowed to add some travel time to their working time. The time being registered by the system is therefore merely a helping tool for the employees to fill in their time sheets themselves. One of our respondents for example, Jan Vet, just came back from a customer in Luxembourg and had to add 14 hours to the sheet. It would otherwise say Jan hadn't been at work at all these days. Also, some flaws occur, especially on checking out of the office. Then the system registers the employee entered, but never left the building, leading employees to maintain all kinds of paper based registries to correct the system. Although employees apparently have a degree of freedom in managing their identity of being at work, they are being tracked in and out of the office which may give a sense of being checked when they fill in their time sheets.

During the implementation of the system, the Workers Council got involved as they received questions from staff members. These questions mainly revolved around what would happen with the information registered by the system. For example: "where is the information stored", "who has access to it", "how long are the data retained" or "is it connected to our desktop phones"? A small number of people argued that the system was a "Big Brother tactic", scanning all their movements through the building. It turned out one specific sales representative triggered these concerns. He was found to have major difficulties with time registration, which is in fact an issue in its own and not linked to the RFID system. Nevertheless, this demonstrates people are likely to use the Big Brother story in relation to RFID. In response Jan Vet and his colleagues checked the implementation with a number of legal advisers and used a checklist of the Dutch Data Protection Authority. Reading this checklist, one can clearly recognise the checklist is derived from the OECD Privacy Guidelines (see introduction).

Jan Vet, member of the Workers Council, stated: "I consider myself to be a quite anarchistic person, but if you describe this system as Big Brother, I think that is a gross statement. You are being followed through your GSM and while you surf the internet. RFID is not much worse than that." Moreover, the system is not used beyond its purpose, for example to evaluate personnel productivity based on their movements or whereabouts. One thing he does worry about is what governments will do now RFID is implemented on such a large scale. "Governments should be liable for not misusing these systems. Their hunt for so-called terrorists should not evolve into permanent scrutiny, which I think is disproportional compared to, say, casualties of car crashes."

Now the system is fully operational and accepted, the Working Council even turned it into their advantage: they use the time registration to prove they are overburdened with work. Like any telecom business, Alcatel cut down on personnel during the recent telecom crash. Now business is improving, the workload is increasing while few new staff are hired. Overwork was claimed to be incidental, but, with the time registration in hand, the Working Council demonstrated is was structural, for some, even beyond the boundaries set by labour laws.

All in all, implementing an active RFID system in order to track personnel may appear quite invasive at first hand, while in practice it has proved to be not so extraordinaire at all. Aside from some practical matters, the system was accepted by the staff quite easily. Jan Vet stated one of the reasons may be that, as they work for large telecoms, they are use to high-tech, high-security environments. Although the system could be used to evaluate the functioning of staff members on the basis of their

movements, but it is not. It remains, above all, a security system. One of the reasons for this may be that the Workers Council was involved in the implementation from the start.

Bringing security in the workplace up to a higher level, RFID systems are currently used in prisons too. Here we can analyse Identity Management on the work floor in its perhaps most extreme form. In this case identities here are not just based on access or presence, but as a monitoring system on the way people move about - prisoners as well as guards. **Penitentiary Lelystad** [case #66] in the Netherlands is one such "smart prison", where RFID not only scans for unauthorised behaviour, but also functions as a reward system.

This prison is especially built for testing new technologies and detention concepts. A maximum of 150 prisoners who volunteered for the new detention concept have a (remaining) penalty not exceeding four months and share a room with five other prisoners. They all carry an non-removable bracelet containing an active RFID chip. Identity and location of the prisoner is tracked in real time. The prisoners can design their individual day programme and the RFID system tracks whether they stick to it, providing information for a crediting and penalty function. An alarm is activated when a prisoner is not following the programme, while they receive extra credits if they do. Although this reward system can be perceived as labour, it is questionable whether this case can be seen as a working environment for the prisoners. For the wards it is and they carry an active RFID tag too, locked on their key-chain.

The wardens chip provides the control room real time information about their whereabouts. It also has a 'panic button'. When there is a problem on the floor, the control room has in instant overview of the wardens' whereabouts and appropriate orders can be given. At first, the prison wardens did not express concerns, nor did they have questions about the technology. After a while however, some issues arose, for instance about what happens if somebody visits the toilets. It seems as though realisation of the possible consequences of the technology grew in time and that examples can help in creating this understanding. In addressing these issues, the concept designer and the prison wardens reached an agreement not to use any information that could possibly be collected with the RFID environment. According to the designer, this has never been the intention and the agreement stands to take away or avoid any concerns.

One Dutch newspaper described the prison is being called 'Big Brother bajes' (bajes is Dutch slang for prison). A visitor of a discussion board commented on an article about the concept: "I also had a major problem with the fact that failure to pay traffic fines or petty theft could land you in a prison like this. That means I, and many others in the class, could have our right to privacy legally stripped from us in a very dehumanizing way if we lived in the Netherlands. I think this kind of surveillance, for petty crimes, is completely backwards of the Dutch, who are otherwise liberal". For now, this person may be incorrect, as both wardens and prisoners have a choice to work or serve time in a conventional prison. But once this pilot proves to be successful and all prisons will use the system, they won't.

All in all, the working environment proves to be an interesting site to investigate Identity Management issues. RFID systems function foremost to ensure that the right people are at the right place. Especially in working environments already focussed on security, more advanced systems enter, leading to new functions for better or worse for both user and maintainer of the environments.

Driving a car: fast access

After work we take our car to go shopping. The first RFID tag we use for managing our identity is the one in our car key. A small passive tag inside the key tells a reader near the lock it is really us trying to turn on the ignition and not someone with a copy of the metal key. We then drive our car to a gas station, which automated payments with RFID readers at the gas dispensers. We then take some toll roads, bridges and tunnels, were our active RFID transmitter behind the front window pay our toll while we drive. In all these accounts, RFID speeds up transactions and provides us access as it defines

our identity as paying customer. Meanwhile, the database of the maintainer of the RFID environments not only registers every transactions, but also where and when it took place. As described in the introduction chapter, this information can be used to profile our movements, which can be very useful for other purposes such as marketing or investigation - with or without our informed consent.

Currently the largest RFID application for paying at gas stations is the **ExxonMobile Speedpass**. [case #131] Although this system is not yet implemented in Europe, more than 6 million Speedpass devices have been issued in the U.S. at 8,800 locations of Exxon- and Mobil-branded service stations. An additional 2 million Speedpass devices have been issued in Canada, Singapore and Japan for use at more than 1,600 locations in those countries. The pass consists of a small black plastic barrel of about 2 cm which can be carried on a keychain. Readers are placed at the pump and in the stores. The RFID chip in the barrel carries a unique code which is connected to the holders credit card account.

The Speedpass is not just used to perform transaction. It has purposes too, such as marketing and investigation. This is clearly stated in the "Privacy Policy" and "Terms of use", which users are assumed to have read and agreed upon when they subscribe to the pass. The form states for example: "Speedpass and its affiliates may disclose any of the information that we collect to affiliates and non-affiliated third parties as described below. We may disclose the information whether you are a current customer or former customer." Among parties mentioned are security services, mortgage banking, direct marketing organisations and "any bidder for all or part of the Speedpass business". In practice this will mean the identity "person paying at the pump", through travel- and consuming profile, could evolve into "potential valuable customer for a motel, mortgage or groceries" or "a potential link to a criminal network".

Once a customer uses the Speedpass for the first time, this act is defined as opting in on this policy. The policy also offers an opt out, but if the information is already passed onto another organisation, ExxonMobile does not have control or responsibility over it. Additionally, users can maintain their user profile on line, e.g. view their transactions and receive receipts on line. An Identity Management issue arising here is one family member tracing another, for example a suspicious spouse. In general, users of this setting have very little control over their Identity Management, while many other parties can build up an identity of them as they like.

Another Identity Management issue is when the Speedpass is not used by its rightful owner. Tags can be lost, stolen or even copied. Researchers at the Johns Hopkins University and RSA Laboratories for example succeeded in reading a Speedpass, cracking the code and reproduce another tag. In order to prevent misuse Speedpass monitors purchase patterns on Devices, and looks for unusual behaviour that may signal unauthorized use. So, comparable to how credit companies operate, Speedpass analyses transactions in real time for awkward profiles. If for example an unusual large purchase is made, or purchases occur at awkward locations, the transactions may be blocked and checked at the rightful owner of the pass.

Meanwhile, as these profiling analyses run real time, one could wonder whether these profiles are only used to prevent fraud, such as direct marketing efforts on the basis of movements and buying behaviour. Still, accounts on its current use indicate otherwise. On on line discussion groups for example, some people express their fear on Big Brother scenarios, but none claim to actually encounter intrusive use of their personal data. Most of the discussion treats mainly evolve around practical matters: at which gas stations it can be used, how the system works and if it really saves time. We encountered similar reactions towards a European system, the French system **Liber-T** [case #108]. Here users pay at the French toll roads, the Telepeage, with an RFID card. The badge gives drivers the possibility to enter and exit toll-routes through specially designed gates, without stopping and paying with cash or bankcards.

The Libert-T pass contains a passive rewritable RFID chip. Fixed data is identification of the bearer, the product (subscription type) and the tag. Modifiable data is observation data on tag status, last entry or exit point and historical data of last 16 entries or exits. Analysing time and place of entering and

exit, travel profiles emerge, which could be of use to the maintainer of this system or other organisations. What do its user think of this? We started a thread on this issue on a forum visited by Liber-T users. One visitor, MarK, draws a comparison between his bank and his Liber-T subscription. He states: “They know my address and my bank account (otherwise payment would not be possible). My bank knows this and there are a lot of other people and authorities that know this too.” He also mentions other ways in which personal information can be gathered, like using your credit card or your cell-phone. Responses from other visitors at the forum confirm his view. Mariette 58 for example thinks it is merely a “characteristic for this age of time”. This argument appears to make up for the fact that “they get to know some things about you”. Moreover, for MarK, being tracked actually gives him a feeling of safety in case he got lost on a French highway. Although it may also be used for marketing, we did not find accounts of people who actually experienced this.

All in all, these RFID applications mainly function to speed up transactions on the road. During its test phase AxxonMobile also tried active RFIDs in cars to speed up the transaction even more. Customers would then only have to fill up their tank, without even waving their card. But that did not work well. At the pump, there are just too many cars and readers in one reading area to distinguish them. Moreover, to most customers it made the transaction a bit too swift, giving them a sense of losing control over it. Active RFIDs however do work well at toll roads. Here an active RFID transponder sends out a signal stating who we are and facilitate a transaction to pay for the road we use. Users may have a feeling of loosing control over the transaction, but the advantage of not having to stop for the transaction probably outweighs this disadvantage and the system is currently used more frequently. Such is the case with the Italian **SI Pass** [case #84]. We already encountered this case when we took the public transport in Turin, but, being promoted as a “card to open all doors” it also pays for toll roads. Not by holding it at a reader when we enter a toll road, but as a key for an active RFID transponder right behind our front window. This transponder can reach a reader somewhere placed at the entrance gate of a toll road, performing a transaction while we continue driving. By inserting the SI Pass as a key to activate the device, we gain control over the communication, preventing covert transactions while we continue our trip.

Most companies who issue RFID payment cards seek to elaborate on the payment function. During the Olympic Games in Turin, the Si Pass could also be used to pay for parking, car rental and bike rental. The Speedpass is also not just to pay at the pump, we can also use it to pay for fast food and groceries at the AxxonMobile convenience stores. During its implementation phase, several trials were held to extend the reach of the Speedpass system even further. In 2001, ExxonMobile started trials at 450 McDonalds in the Chicago area and in 2003 with Stop & Shop supermarkets to see whether the pay system could be extended to fast food and groceries. According to Joe Giordano, vice president of systems en product development at Speedpass their customers expressed the need to use it at other “around-the-town, convenience oriented-type purchases”. Still, for some reason or another, these applications never past the trial phase towards the broader public. It seems likely RFID systems do have their limits when it comes to payments, as will be confirmed by our experiences in shopping. In this setting major fear was evoked once people discovered both their groceries as well as their customer loyalty cards were tagged.

Shopping: tagged items and customer loyalty cards

In the short history of RFID one application perhaps stirred most controversy: tagging groceries. It started with the aim to gain efficiency in the supply chain by replacing bar codes in crates, pallets and boxes with RFID tags, as happens in many logistic chains today. As soon as the price level of a tag dropped sufficiently, the next logical step seemed to be item level tagging: an RFID chip to identify single products uniquely. With an unique code, the product could identify itself all the way from production, distribution, to sales and even beyond. Notorious future examples were smart refrigerators to tell whether the milk was due or intelligent washing machines to set the temperature according to the tags in clothes. But this did not happen. Item level tagging in supermarkets displayed a very

sensitive link in the chain: customers intent on taking their Identity Management into their own hands. Early examples come from the US, where CASPIAN addressed the Identity Management issues concerned with item level tagging at Wall Mart supermarkets. In Europe the German FoeBud triggered a controversy on the Metro Future Store when item level tagging was combined with RFID customer loyalty cards.

The **Metro Future Store** [case #4] is a supermarket of the German Metro Group where new technologies are tested in a real setting. RFID was first of all used in supply chain management. Cartons and pallets were tagged and readers installed at the exits and entrances of distributions centres and the warehouse. In 2003 the supermarket started experimenting with tagging groceries individually. RFID readers incorporated in shelves and connected to the central supply chain management system could then scan the tags of individual products. For the supermarket personnel, the main functions of item level tagging are stock-control, checking for misplacement and quality control. In order to prevent the tags from being read by any third persons once the customer leaves the store, these tags are supposed to be disabled by a de-activator at the exit of the store.

For the customer, the so called smart shelves also provide product information triggered by the item tag. Customers can go to an information terminal to see which data is stored on the chips. An in-store service to view or listen to trailers used tagged video and audio products. German law however demands this occurs according to age limits set by the industry. The trailers can therefore only be activated with the RFID tag in the customer loyalty cards, checking whether the customer has reached the appropriate age to see or hear the trailer. At that very moment, the identity of the customer and the product were be linked.

Once the RFID system was operational, the Metro Future Store invited customers to test it. About a year after the opening of the Future Store, FoeBud protested against RFID in the store. Main issue was the coupling of information about customers' age on the RFID enabled loyalty cards to video and audio products, when using the in-store viewing service. According to Albrecht von Truchseß, a Metro spokesman, this was done to meet German law on age restrictions. Still, according to the protesters, Metro did not inform its customers their loyalty card contained an RFID too. Besides the matter on RFID loyalty cards, several other possible applications are being targeted by privacy advocates. One was on the possibility of RFID enabled shopping carts to track customer movements. Also, the RFID tags should have been de-activated at the exit of the store, but the device malfunctioned on several occasions, leaving the tag open for intrusion outside the store.

In our correspondence with Metro, all these fact were refuted. Daniel Kitscha of the Corporate Communication department claimed customers were informed about the presence of RFID in their card orally and by a brochure. Also, only customers of age 16 and up could receive the card, which automatically puts up the age barrier for previewing movies. Further, the tagged shopping cart was also a fable: there was only one prototype cart with an RFID *reader* to scan for groceries, which was never actually used. Finally, he claims there was no negative public response towards RFID, not in their surveys and not on their customer hotlines.

Nevertheless, due to this controversy, the Future Store was forced to recall the loyalty cards and restore barcode systems. Some handbooks on RFID (e.g. Garfinkel, S. & Rosenberg, B. 2006 or Van Trier & Rietdijk 2005) as well as many policy documents still mention Metro as one of the examples in which Identity Management went totally wrong. This is an image hard to counter by any good intentions of the supermarket. For now, Metro remains determined to keep RFID technology in the supply chain. Mr Van Truchseß said. "A top priority is the use of this technology for tracking pallets and cases. And although we're still interested in testing the technology at the item level, this isn't a priority at the present." We saw this precautious behaviour with two other retailers too. They did implement item level tagging and took careful notice of the controversial aspect of connecting item level tags to customer identity.

In spring 2006 **Marks & Spencer** [case #6] implemented RFID item-level tagging using the 'Intelligent Label' for a trial in 53 stores. The RFID system keeps track of in-store inventory and ensures that a full range of sizes of any product is available to the customer. During an earlier small-scaled pilot the Intelligent Label was attached to the product alongside the pricing label and designed to be cut off and thrown away after purchase. In the extended trial, the tags were not used in the purchase-process, but only read throughout the supply chain and in the store for stock taking. Therefore the RFID inlay was embedded into a single label that also carries a bar code and a text informing customers: "Intelligent Label for stock control use".

During trial design and implementation, Marks & Spencer consulted privacy groups on possible privacy implications. These efforts led to positive reactions among sceptics. C.A.S.P.I.A.N. for instance acknowledged that Marks & Spencer has taken a socially responsible position. Despite these positive sentiments, C.A.S.P.I.A.N. denounced the trial in a press release, saying it does set a dangerous precedent by putting RFID tags in clothes. Another privacy watch group, spy.org, claims the message on the labels mentioning "Intelligent Label for stock control use", have recently been removed.

The retailer has opted for minimal customer-directed use of the tag, avoiding privacy issues, and has taken efforts to inform its customers. In the brochure about the RFID tags, Marks and Spencer states that the label does not have a battery, is harmless, can be thrown away after purchase without losing the right to refund or returning and will not be scanned at checkout. Instead, barcodes are scanned. This way, no link is made between the product and the customer, regardless the method of payment. Our last retailer, **Selexyz Bookstore** [case #35] also took care to strike the right balance between providing personalised product information and securing privacy. In this case the balance may be even more important, as their products do not consist of perishable goods but information.

Selexyz bookstore in Almere, the Netherlands implemented an RFID system mainly for efficiency reasons: make the supply chain more transparent, improve stock control and reduce labour costs. The system should also enrich customer experience and increase sales. Each of its 38,000 books carries a unique code, which can be read by mobile and stationary readers throughout the store. An employee for example places an unopened box with RFID tagged books into an RFID 'tunnel', which is equipped with a reader. This checks the tags against an electronic record of an advanced shipping notice forwarded earlier over the Internet by their supplier Centraal Boekhuis. If there is a discrepancy, the system automatically sends an alert to rectify the order. Checked-in books are placed on store shelves and other displays, with their exact location scanned by employees with handheld RFID scanners. This gives clerks and customers an instant look at a book's exact location as well as its availability.

Customers can use the RFID system to retrieve information on the whereabouts of a book through the information kiosks in the store. Selexyz also offers the possibility to place orders, when the requested book arrives the customers gets a notice by e-mail or text message. When we bought a book at the store, we were surprised to find out it does not only contain an RFID chip, but also a bar code which is scanned at the moment of purchase. Having these two systems side by side does not appear to be very efficient but it is all meant to prevent controversy as described in the Metro case. The company took several other measures to prevent privacy issues. They proclaim not to link purchase information with specific customer information and when a book is bought, the chip is deactivated by store personnel.

However, it is not clear whether future applications of the RFID environment will be part of marketing strategies. For instance, a member of the management board of BGN mentioned the possibility to link the tags to screens in the shop to display information or advertisements. Naturally, it is not prohibited to use smart marketing techniques in your own store, but this method seems to be somewhat more invasive, with screens lighting up when a client picks a certain book from a shelf. Currently, the store has no such displays. In fact, the customer hardly notices the tags and only the leaflet on the RFID tags reminds of their presence

All in all, there is not much going on concerning Identity Management when we go shopping. Perhaps because it were in fact these settings in which the first big controversies emerged, not only in Germany but also in the US, the sector became very cautious linking RFID to customers identity. For now we are done shopping and it's time to have some fun. We can go to a theme park, football match or a night club, to discover RFID is sometimes used to track us as crowds, but also to give us personalised privileges.

Having fun: privileged persons and tracked masses

The leisure sector turned out to be the most surprising in our research. Other than in retail, we encountered many interesting stories on Identity Management, some being widely discussed in the media, while others only unfolding within the secured boundaries of the leisure setting.

One case receiving some media attention is the **LEGO land KidSpotter** [case #36] in Billund, Denmark. At the entrance of the park, parents can rent a wristband containing an active RFID for their children for € 3,- a day. Throughout the 150.000 square meters park about 40 to 50 RFID readers are placed. If the parents lose sight of their child, they can send an SMS message to the KidSpotter system. They will receive a return message stating the name of the park area and the map coordinate of their child's position in the park with an accuracy of 3 meters.

This security function is the main reason for parent renting the wristband, countering the problem that about 1600 children get lost in the park annually. Identity Management in this case involves a combination of personal identity, place and phone number. Some newspapers hypothesised parents could also just drop off their children at the park and go shopping elsewhere, trusting their children would be confined within the area, but we are not sure this actually happens.

From the parks point of view, another Identity Management opportunity arises: tracking the flow of visitors through the park. The readers divide the park up into a number of areas and the database shows the number of people in each area and how many move from one area to another. This is valuable information, for instance for the marketing or catering departments. We contacted several spokespeople at LEGO land, but none of them was willing to give us more details on Identity Management issues in the park. One even claimed the system was abandoned, but according to its provider, KidSpotter, it was not. We therefore went to a theme park in the Netherlands which also tracks visitors with active RFID, but this time without them knowing.

The **Apenheul** [case #130] is a zoo specialised in all kinds of apes and monkeys. An outstanding feature of the park is the opportunity for some kinds of monkeys to move freely through the crowd of visitors. Curious as they are, the monkeys often try to open visitors' bags in hope of a free lunch. The park therefore introduced the "Monkey bag", a green bag with an extra clip lock which monkeys cannot open. The bag is obligatory, which is enforced by the receptionists providing the bag at the entrance of the park and a warning sign. Aside from this security reason for implementing the bag, the department of marketing added a marketing feature to the bag: scanning visitors movements through the park through an active RFID sewn into the bag.

Currently about 200 of the 3000 bags are tagged. In order to provide a representative sample of visitors, the tagged bags are handed out random, adding to 1 in 15 visitors tracked. A dataset of 90.000 readings provided the data to analyse for visitors flows. If for example an area receives too few visitors, it presumably needs to be made more attractive. If the area receives the most visitors, it's probably a hit. Also, if visitors demonstrate a pattern of "getting lost", e.g. moving back and forth a lot between two areas, the directions need to be changed. Finally the overview of visitor flows can detect congestion spots that need to be relieved.

According to several park hosts, visitors were informed about the presence of the tag during a pilot phase, but this policy has changed as people then may refuse the bags. Marketing manager Smit remarked afterwards there is no reason to inform the visitors on the presence of the tag as it does not gather personal data, only anonymous movements. The Apenheul therefore complies with data protection laws. Jochem, the park host who recollects the bags at the exit, receives questions sometimes from visitors who discover the tag (it's tangible, about 4 to 10 cm on the inside of the bag). Visitors react surprised, according to Jochem, but never with much discontent.

This case touches upon the issue on what are personal data and the control costumers should have over data retrieved from their movements. The Monkey Bag RFID has a marketing function: how do visitors move through the park and how can the flow of people be optimised. Visitors are being traced without informed consent. The tagged bags are provided without informing it's user on the tractability. Moreover, the use of the monkey bag is obligatory. Visitors are given a bag at the entrance with a security argument "Monkeys move freely through the park and will try to steal your goods." Although legitimate in itself, this rule limits the free choice of the visitors not to use the bag.

Still, the visitors remain unanimous, are not traced real time and do not suffer any consequences as a result of the data they provide. In that sense, the data retrieved cannot be seen as an identity that should be managed from a user perspective. Bert Smit, the marketing manager who leads the implementation, says it is exactly for this reason that his visitors tracking system complies with the law on protection of personal data. But aside from the law, one may wonder how visitors will react once this story gets out in the open.

Being profiled on movements can be experienced by some as invasive, while for others, it can also give a feeling of being privileged. Imagine 50,000 people in a building who will do just anything to manage their identity as being part of that group. Add to this a maintainer of that building who has to identify those who are or are not paying, consuming, being loyal and behaving well - all this in a matter of just two hours. This is the case at the **Madejski Stadium** [case #88] in Great Britain, which calls itself a "smart stadium" using among other ICT applications RFID tickets. The ticket system not only provides access to the stadium, but also serves as a customer loyalty, payment, crowd control, security and direct marketing application

The RFID system was initially implemented at the Madejski Stadium in 2004 for security reasons: to limit access to valid ticket holders only and to control the number of people in the stadium. Tags are passive and used in plastic RFID cards (member cards and season tickets) and in one-off paper tickets. RFID readers in all the turnstiles administer access to valid ticket holders. Service personnel throughout the stadium carry pocket computers (PDA's) which are linked to the central database through a wireless network. This database can be accessed through entering the card number (not through RF!), providing the full identity of the card holder: ID-number of the card or ticket, name of the carrier, time of entrance, status of ticket (e.g. access to which game and through which entrance), status of carrier (e.g. blocked card, watch-listed or black-listed person) and area and turnstile of entrance. Besides the RFID tickets, Closed-Circuit television (CCTV) is used to feed the information system. For example taking pictures of supporters or to supervise the ground. Together with the ticketing system, the stadium knows exactly who is sitting at a certain seat. When a supporter is not following the rules or is having a dispute with personnel, the CCTV system can serve as proof and adequate action can be undertaken.

At our visit to Madejski stadium IT manager Mr. G. Hanson, informed us the function of the club card will be extended as a payment system, a so called e-purse system. The e-purse is a debit card to pay for example for parking, public transport to the stadium and consumptions in the stadium. The system not only facilitates the transactions executed at the ground, it also gives the stadium management insight in the expenditures of each supporter. This way they can see who are the clubs' 'big-spenders' and link this to their Customer Relation Management scheme. This means the stadium management is actively approaching its most loyal visitors, giving them special offers on their birthday or priority on

popular matches. They can also be approached if for example they did not renew their season ticket or did not buy a new T-shirt that year.

A smart stadium indeed, but what do the fans think of this? During our visit, one member cardholder commented on the fact his whole history is retained and analysed: “It is good that they can see who are the better supporters.” Another mentioned: “It then helps keep good fans in the club and get rid of troublemakers”. A third regular mentioned: “Yes this is good so you get a benefit for attending more matches.” Still, the fans do have one worry: the use of information by third parties. This should not be allowed according to them. One person says they do not have any experience with non-football related marketing, but are not certain if this will remain like this: “But they probably also use personal information for marketing purposes. What can you do about it? You can not prove it and you can not change it”. Another supporter states he would want to have a say in the applications for which personal information or the information gained through the RFID system is used and that he would not want any third party being involved or benefiting from this. According to Mr. Hanson, the information gained in the RFID environment is only used for in-house purposes. The stadium can and will not trade the information to third parties. For one thing, the Data Protection Statement of the register procedure prohibits this and this and other issues about privacy are covered by British Law.

The Fortress system is currently in use in many British and Norwegian football stadiums and we found accounts of comparable systems in other countries. Although these systems can be seen as being very invasive, taking full control over a persons' Identity Management within a stadium setting, we did not encounter any public controversy. One controversy we did encounter in football was on a ticketing system which was even less intrusive concerning tracking people, but was just of a different league: the World Cup 2006 in Germany.

Football fans who attended a match at the football world cup in Germany got their ticket through the **FIFA World Cup ticketing Centre** [case #19]. These tickets contained passive RFID tags in order to combat counterfeiting and to ensure only those with legitimate tickets can get in. On applying for a ticket one has to provide personal information: name, address, nationality, sex, date of birth, passport number, e-mail address (optional), telephone number (optional) and, possible, also the club you are supporting. This information is stored in a database and linked to the ID-number on the chip. The chips were only scanned at the entrance of the stadium, while there were no scanners inside the stadium or anywhere else. The data however, are shared with third parties such as security agencies, stadium operators and shipping providers if necessary, as is stated on the FIFA website. This led some privacy groups to accuse Germans football authorities of “Big Brother tactics”. Foe Bud for example stated that the RFID tags are being justified under false pretexts, like security reasons, and that it is unfair to insert this kind of technology in an item that much wanted by fans.

> “What could be nicer: A top-event with millions of enthusiastic people who would do just about anything for their most beloved hobby. Add to this a September 11 heralding no end of "threat by terrorism", and you have all the justification you need for just about any measure to cut down on freedom rights as long as there is a sticker on it saying "security". And should the World Cup go past without any assaults you have every justification to afterwards call the whole "security-concept" a success, RFID in the tickets and all, and silence all the critics with a hearty salute: "Hey, all of you conspiracy theorists, hundreds of thousands of soccer fans didn't have any problems with RFID!"

Another group entering the debate was the German Data Protection Centre. They state on their website that supervision and security are two different things. Therefore, introducing technologies under the pretext of enhanced security cannot be done just like that. According to the FIFA however personal data are processed in compliance with the Data Protection Legislation. Moreover, compared to the other cases in football, this RFID system is not as much intrusive as it only tracks the user at one point: the access of the stadium. Still, it was the privacy watch groups which led the debate over this case. Our final case in the leisure sector did involve a much broader public debate, urging not just privacy groups, but also a whole host of journalists and even parliamentarians to participate. Not

because people were tracked without knowing or disproportional, but because of the way in which the RFID chips are carried: inside human flesh.

Barcelona (Spain) and Rotterdam (the Netherlands) are both host of a leisure branch called the **Baja Beachclub** [case #18]. While the Barcelona club actually resides on the beach, the Rotterdam club creates a beach atmosphere in a concrete environment with all sorts of water attributes such as water scooters, palm trees and jacuzzi. Personnel is dressed in swimming clothes. Next to the bar there is a VIP deck, were fancy drinks and snacks are served. This is the area of loyal customers who carry an RFID implant in their upper arm which serves as an access code and digital wallet to pay for drinks. The cost of the chip and the resulting membership is € 1,000, while the club places a credit on the chip of € 1,500 for drinks.

According to Conrad Chase, director of the Baja Beach Club Barcelona, the chip was introduced for two reasons. First, for the image of the nightclub, they wanted to offer their guests an original item. Second, to benefit from the latest most advanced technology, something that could offer convenience for both the nightclub as well as the carriers. His Dutch colleague Jo van Galen adds to this that the carriers regard the chip as a special gadget that supports the VIP treatment in a positive way. It's not just they do not have to show identification or have to handle money, but it's moreover the feeling of being an appreciated guest of the club.

The Verichip was initially developed for medical purposed, to identify patients. It consists of a glass tube the size of a grain of rice containing a passive RFID with a single fixed code. It is implanted in the upper arm with a needle. Before implanting the chip the VIP signs a statement of free will. This statement also contains an acknowledgement that the chip and the information will remain property of the nightclub and the carrier can decide to have the chip removed any time and without former notice to the nightclub. When they go to the club, VIPs have their chip read at three moments: on entering the club, on entering the VIP deck and when paying for drinks. Club personnel read the chip with a portable reader which displays only the ID-number of the chip. This number is transmitted to the central computer and details of the customer are displayed on screens which can be accessed throughout the club. These details involve: name and photo of the carrier, balance on the chip and transaction history. The transaction history consists of transaction amount, time of transaction and bartender running the transaction. No information goes outside the club.

The club uses the system as an informal loyalty system, however the technology is not a key-instrument in this; it could also be done without, based on personal experiences with guests. Regulars and 'big-spenders' get offers like first options to limited tickets, invitations to special nights and Mr. Van Galen even mentioned offering a airplane ticket to a Spanish guest. Guests regard this loyalty scheme as positive, according to our respondent. The Rotterdam club currently has 70 people who carry the chip. Manager Jo van Galen explains that the number will not be increased, because it has to remain an exclusive thing. Interestingly, most of the chip carriers are men, about 80%. Van Galen explains: "A VIP can also invite two other persons to the VIP deck. Women want to be invited to the VIP area, whereas men want to invite women."

From the perspective of Identity Management, this case can be seen as quite normal: user and maintainer of the system mutually agree upon what kind of information is used to what purpose and no other parties are involved. As the user receives extra VIP treatment and extra credit for drinks, it can be seen as an extended version of a customer loyalty scheme. Still, due to the method of implanting tags, this case triggered huge debates. Some journalists compared the tagging of VIP to the tagging of cattle. Privacy groups claimed it set a president to use implants for other purposes too. Some Christians regard the implant as unethical, referring to biblical sections on the arrival of the beast, which should be preceded by people being marked with a number. In the Netherlands, the issue went all the way up to Parliament, where a spokesperson of the Christian Union Party opened the debate on whether it should be allowed to tag people in this way.

Barcelona director Chase foresees a future in which everyone will have an RFID implant: “the objective of this technology is to bring an ID system to a global level that will destroy the need to carry ID documents and credit cards. The VeriChip that we implant in the Baja will not only be for the Baja, but is also useful for whatever other enterprise that makes use of this technology.” One of the VIP guests of the Baja Beach Club Rotterdam, Steve van Soest agrees: 'The main benefit is that you can go out without having to carry a wallet, which can get easily lost in a night club. […] It would be great if this catches on and you could put all your personal details and medical records on it. If I was involved in an accident, doctors could simply scan me and find out my blood group and any allergies.' The director of the Rotterdam club, Jo van Galen, has a more reserved view on the application. He recognises the multiple opportunities the technology has, but is cautious about expanding the applications of the chip. His main concern is running a business, while the Dutch society and media tend to portray the Verichip in a negative manner. Consequently Mr. Van Galen is very much aware that opinions on the technology can change easily from positive to negative and that this can harm the nightclub’s image.

Still, Van Galen foresees some future applications too. Such as chipping personnel. Currently, personnel of the nightclub carry tokens with chips in them. This way they can enter through a personnel entrance. However, the token could be transferred to another person. The implant could have a big advantage there, since it cannot be transferred nor lost be the carrier. But it should not, as we have seen on the section on working environments, be used for time-registration. Mr. Van Galen also thinks about using a credit system in stead of the current debit system. This will involve linking the ID of the chip directly to a bank account or credit card. An advantage could be that a guest would never have to hand over any cash or bankcard and may enhance the feeling of exclusiveness. A disadvantage could be that it does not ‘protect’ a guest from spending more than intended, since there is no maximum amount to spend. Furthermore, it involves issues of privacy and safety. Finally Van Galen is in favour of the application expanding to other nightclubs. He envisions a ‘chippers-community’ in which VIP Chip carriers from different nightclubs can meet (in person or virtual) and in which they can use their status in associated clubs. For now, the chipping community will remain inside the Baja Beachclub until the negative storm of publicity surrounding the chip has settled down.

Crossing Borders: automating recognition

Continuing our travel, we will now take a plane from Amsterdam to Paris. At checking in, two RFID chips are managing our identity: one to track our luggage and one to prove we are who we claim to be. The first one is easy from our point of view: in stead of a bar code strip, the hostess connects an RFID to our bag. From the perspective of the owner of this setting, the new system is a massive operation which will make luggage handling faster and easier. The second application, our RFID passport is perhaps the most complex Identity Management operations in the history of RFID. The chip does not only store a unique number, but also picture of us. In the future, fingerprints will be added. In order to secure only the legitimate owner of the RFID environment can read the chip, many complex security measures need to be taken.

In 2004 the the International Air Transport Association (IATA) launched a programme to test and build a business case for the use of RFID for luggage management. In November 2005 the organisation introduced a global standard for RFID baggage tags. **Air France-KLM luggage handling** [case #15] serves as a test site on flights between Paris-Charles de Gaulle and Amsterdam Schiphol Airport. Later in 2006 more drop-off points in Amsterdam Schiphol Airport will be using RFID labels. The goal of the pilot is to improve the baggage handling process. By implementing RFID labels more reading points are possible, due to automated reads and a higher read rate than bar codes. Thus, bags can be sorted and loaded faster than bar code systems and the number of mishandled bags and associated costs is reduced. For now, the pilot looks promising from the point of view of Identity Management. Bags can be identified easier, while the code can also be changed, for example when a flight direction is changed. From the perspective of the traveller, one may suggest this new system

does not involve any Identity Management issues. Still, we did find some accounts on on-line forums of people who worried their bags may be read by unauthorised persons or others may distort the database by deploying chips in their bags with false IDs. For now, this case is still unfolding and there are no issues yet. Accounts of unauthorised readings or even falsifications of the **RFID passport** [case #23] however are alarming, as we will see in the next case.

Europe has just past the deadline of 28 August 2006, on which all European countries should have implemented the biometric passport. The following countries made it: Belgium (November 2004), Sweden (October 2005), Germany (November 2005), Great Britain (April 2006), Austria (June 2006), Denmark (August 2006) and the Netherlands (August 2006). Following demands from the U.S. Visa Waiver Program, the ICAO (International Civil Aviation Organization) decided in May 2003 to use facial recognition in travel documents. The European Union followed in September 2003 with the decision to use a photograph and two fingerprints. The technical specifications were determined on the 28th of February 2005. At first only digital photographs will be saved on the chip inside the passports. Later additional biometric data can be added, such as fingerprints, DNA-profiles and iris-scans.

The main reason for going from paper-based to an RFID passport is to combat look-alike fraud. With the former passport, anyone who would resemble the picture in it or succeeded in replacing the picture with their own could take the identity of the rightful owner. With the RFID passport, the picture is not just visible in the document, but also stored on the chip in a universal format. Border control officers can then check whether the visible and electronic picture matches. Cameras can also analyse the facial structure of the person holding the passport and compare this with the electronic picture. Another, more practical reason for using RFID is to speed up border control: the passport can be read automatically, cutting down on time for manual checks.

Many technical measures have been taken to secure the communication between reader and RFID, such as Basic Access Control. The chip can then only be read if the passport is opened and placed on the reader, which reads the text printed on Machine Readable Zone. The text contains the name, country and passport number of its holder and also serves as a key to start the communication with the RFID chip inside. Advanced as it may appear, researchers from the Radboud University Nijmegen [Hoepman et al 2006] succeeded in eavesdropping on the BAC procedure ("skimming") from a distance of several meters by guessing the 128 bits on the MRZ. Normally, guessing a code of that size would be merely impossible, that is, if it were a random code. The MRZ however is not random, but contains certain information which can be expressed in formula, drastically bringing down the range of possibilities. For example the issuing date and expiring date are limited and logically connected. Some countries issue the passport numbers sequentially, again establishing a link with issuing date. The researchers cracked the code and could read from a distance who was holding the passport.

The European Union therefore stepped up to Extended Access Control in which not only the passport but also the reader needs to identify itself with a certificate. The Raboud researcher's state this is a major step forwards but still doubt whether it will work in practice. Reading machines will probably be stolen, breaking the security chain. This will be countered by issuing temporary certificated, but the current chips don't have a source to measure time. Also, managing a large international issuing system for certificates will lead to mayor overhead.

Another leak in the system also appeared when it turned out different countries use different RFID chips. It would for example be possible to distinguish from a distance between Europeans and Americans, without going through the Basic Access Control procedure. One hypothesis, occurring in the media quite often, is a smart bomb placed in a public space, being set off at the moment a certain number of passports from a certain country are near. Although this may be possible in theory, it has not occurred yet. But people are already taking precautions by shielding off their passports with metal covers, preventing unwanted communication with readers.

These issues can be seen as the technical side of Identity Management. From the users perspective a much more personal Identity Management issue arises: governments using the passport for much more

than just border control. Although this is mainly triggered by the biometric database and not by RFID, contactless communication facilitates the exchange of biometric information and is therefore also seen as responsible. One such function added to border control is that the biometric database will itself be an analyses tool. For example: searching for potentially hazardous people on the basis of their appearance. A picture can for example tell much about someone's religion or race. Another function creep involves connecting the central database to other databases, getting a full picture of a person whereabouts and being sure the person actually is who they appear to be. It's for this reason organisations such as the Dutch Data Protection Authority are opposed to a central database for the biometric passport. Also, many reactions in newspaper claim the biometric passport is just another step towards a Big Brother regime. Put more subtle, the Radboud researcher's state:

> "The possibility of biometric identification of the entire (passport-holding) population involves a change of power balance between states and their citizens. Consent or cooperation is then no longer needed for identification. Tracing and tracking of individuals becomes possible on a scale that we have not seen before." [Hoepman et al 2006: 11]

They expect some political groups will be likely to combat the RFID passport. These groups could for example persuade people to put their passport in the microwave, destroying the chip while saving its physical appearance. Even stronger, such a political action group could build disruptive equipment to destroy the RFID-chips from a distance without the holder noticing. Yet, as for now, citizens are complying with the new passport. Identity Management issues from the side of users are currently mainly on practical problems with biometrics, as it took many people much effort to get their picture right. They had to look straight into the camera and were not allowed to smile, which gave them a feeling of being squeezed into a uniform format. Also, early tests show facial recognition does not always work well, especially with children and elderly.

Once the majority of the European population has an RFID passport, new, perhaps unanticipated applications may be suggested. Being the ultimate Identity Management application, banks, insurers and other organisations would want to use it too to manage the identity of their customers. How Europeans then try to take Identity Management back into their own hands remains to be seen.

Taking care: informed medics, securing patients

Finally, one setting which could be part of everyday life is being taken care of by medical specialists, both in the hospital environment as in homecare. When it comes to RFID in a healthcare setting, almost everything can be tagged for some purpose: assets, patients, pharmaceuticals, blood bags, laboratory samples and staff. With item-level tagging Real Time Locating Systems can be used. In the case of assets and staff for instance, this is done for theft prevention and rapid location. The tags can also serve as an 'electronic handshake', making sure the right procedure is followed. Patients, pharmaceuticals, blood bags and laboratory samples are tagged for this purpose of error prevention. Furthermore, tags on pharmaceuticals function in anti-counterfeiting. In addition a newborn and his or her mother can be tagged for mother-baby matching. Finally, patients could tagged for drug compliance and supervision of the cognitive impaired. [Harrop, P. & Das, R., 2006; Garfinkel, S. & Rosenberg, B. 2006] Nevertheless, although many possible uses are being developed and in some cases tested, we found very few actual accounts of RFID and Identity Management in healthcare settings. Tagging items has become quite common, mainly for logistic purposes, but for some reason or another, identifying patients with RFID is not (yet) common practice.

One case we encountered in Imatra, Finland. Here medication compliance is controlled by the **Medixine RFID Communication Board** [case #133]. People suffering from Alzheimer's disease are enrolled in the trial. According to Medixine they are suitable for this application, because they have no problems in administering the medication, but they need a reminder to do so sometimes. The RFID

Communication Board device is equipped with a number of RFID tags, each assigned to specific situation. Situations can be for instance 'I have just taken my drugs', 'I feel lonely' or 'I need help immediately'. A situation can be activated using an mobile phone which uses RFID signals. This message is then broadcasted over a network and compared to the patient's record; if necessary other people, like a doctor, a family-member or a friend, are informed. Patients learn to use the system when they are still in an early stage of Alzheimer's disease. When their condition deteriorates, they still remember to use the communication board. In this case, the patients' condition makes strict supervision by a medical team necessary as patients are not capable of taking care of themselves in certain situations. The technology brings this supervision as far as in people's own houses, be it in a rather inconspicuous way. On the other hand, without the system, the patients might not even be living in their own houses anymore.

Trials were patients and items that are part of their treatment are tagged, appear to be more common in Europe, for instance in the Ospedale Maggiore in Bologna, Italy and in the Klinikum Saarbrücken in Saarbrücken, Germany. When a patient arrives at the hospital he or she receives an RFID bracelet. This bracelet makes it possible for hospital staff to identify the patient and to access medical records quickly and apply treatment with more accuracy. Also, blood bags are tagged by the hospital. All patient records and blood supply information are held on a secured database, which can be accessed by medical personnel through a PDA. Medical records are constantly updated, based on the reading of the PDA's. In Italy, there is an extra security measurement: only after a fingerprint-based biometric authentication is completed a person can read the identifications of the patient and the blood unit being used in any transfusion. If the unique identifiers on the patient and the blood unit are a match, a wireless electronic seal on the blood unit is released, permitting the transfusion to occur. A similar trial is also being executed at the Amsterdam Medical Centre in Amsterdam, The Netherlands. Besides matching and error prevention of blood transfusion materials, individuals working in the operation rooms (OR) are identified and localised, as well as OR-materials.

Our search for interesting stories on the use of RFID in everyday life has taken place in a variety of settings: travel, leisure, work, shopping, border control and health. We encountered most Identity Management issues when we were on the move: in public transport, while driving our car or when we crossed borders. The leisure sector and working environment turned out to be fertile testing grounds for many new applications. We have found that retail and healthcare deploy RFID mainly for logistical reasons, with some accounts of Identity Management. In the case of retail many maintainer appear cautious because of concerns over customer reaction while the use of RFID in healthcare is still in its infancy. These settings demonstrate that the roles users and maintainers play depend highly on the setting. In the next chapter, we will summarise these for each setting.

Discussion: multiple identities in smart environments

This research report will provide input to several sessions taking place in the next phase of this project. During these sessions we will develop scenarios for the settings described above: which identities are attributed to users of RFID environments by the owners of that environment and users themselves? Sometimes third parties are involved too, such as governments or marketing organisations. As a kick off for these sessions, we draw an extraction from our case studies for each setting.

Public Transport

Users' identity defined by…		
User: I am …	**Owner: this users is …**	**3rd parties: this user is …**
• a ticket holder • a frequent user • pretending to have paid while I have not (fare dodging) • being an anonymous traveller	• a ticket holder • travelling during peak hours • taking certain routes frequently • specifying trips before or afterwards • fare dodging • a customer for additional services	• a potential criminal (police) • a potential witnesses of a crime scene (police) • a potential customer (marketing) • my unreliable spouse (partner)

Work

Users' identity defined by…		
User: I am …	**Owner: this users is …**	**3rd parties: this user is …**
• Having legitimate access (place, time) to certain areas • Being at work • Gaining higher access levels • Working overtime • In danger during emergencies • Having entered but never exited the building • A guest	• Having legitimate access (place, time) to certain areas • Present/productive • In danger during emergencies • Near colleagues or devices • In an area while not allowed • A guest	• In danger during emergencies

Roads

Users' identity defined by…		
User: I am…	**Owner: this users is…**	**3rd parties: this user is…**
• a paying customer having access • preventing others to use my account • preventing links with other purchases (fast food)	• a paying customer • a potential customer for additional services • Combining acquiring gas or toll with consumption of certain products	• a potential customer for additional services (businesses) • a potential criminal (police) • an unreliable spouse (partner)

Shopping

Users' identity defined by…		
User: I am…	**Owner: this user is…**	**3rd parties: this user is…**
• a paying customer • of a certain age and allowed to consume this content	• stating preferences by combining certain kinds of products • of a certain age • shoplifting • moving through the store in a certain way	• a potential customer (other shops) • shoplifting (police)

Fun

Users' identity defined by…		
User: I am…	**Owner: this user is…**	**3rd parties: this user is…**
• a paying customer • of an undisputed reputation • being a loyal customer/fan • having privileged access (tickets, areas) • getting extra free products • lost	• a paying customer • a "big spenders" • lost • part of a congesting crowd • behaving well or badly	• a potential witness (police) • behaving badly (police) • spending much money on leisure activities (social services)

Border crossing

Users' identity defined by…		
User: I am…	**Owner: this user is…**	**3rd parties: this user is…**
• who I claim to be • a citizen of country X • allowed access to country Y	• who he/she claims to be • is citizen of country X • allowed access to country Y	• potential criminal (police) • member of a certain religion a or race (police) • citizen of country Y (terrorist)

Healthcare

Users' identity defined by…		
User: I am…	**Owner: this user is…**	**3rd parties: this user is…**
• receiving the right medicine at the right time • the mother of this child • a doctor being at the right place on the right time	• receiving the right medicine • mother-baby match • a doctor being at the right place on the right time	•

Sources

Sources on specific case studies are described in the case study templates. These are the general sources used throughout the report.

Literature

Balkovich, E., Bikson, T. & Bitko, G. (2004) *9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace.* Los Angeles: RAND Corporation.

Capgemini (2005) *RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business.*

Garfinkel, S. & Rosenberg, B. (ed.) (2006) *RFID: Applications, Security and Privacy.* Addison-Wesley. -555p.

Harrop, P. & Das, R. (2006) RFID in Healthcare 2006 – 2016: report summary. IDTechEx

Leisner, I. (ed.) (2006) *RFID from Production to consumption: risk and opportunities from RFID-technology in the value chain.* Copenhagen: Teknologirådat. -12p.

Locquenghien von, K. (2006) 'On the Potential Social Impact of RFID-Containing Everyday Objects.' In: *Science, Technology & Innovation Studies,* Vol. 2 March 2006, pp. 57-78.

Nsanze, F. (2005) *ICT Implants in the Human Body.* European Group on Ethics in Science and New Technologies.

POST (2005) "Pervasive Computing" POST note May 2005, no 263 of the Parliamentary Office of Science and Technology

Retail Systems Alert Group (2004) *RFID: How Far, How Fast: A View From the Rest of the World.*

Rodotà, S. & Capurro, R. (2005) *Ethical Aspect of ICT Implants in the Human Body.* European Group on Ethics in Science and New Technologies.

Schermer, B.W. & Durinck, M. (2005) *Privacyrechtelijke aspecten van RFID.* ECP.nl

Schermer, B.W. (2006) *RFID & Privacy voor managers.* Platform Detailhandel Nederland, ECP.nl, RFID Platform Nederland

Thomas, A. (2004) 'Radio Frequency Identification (RFID).' In: *Postnote*, no. 225.

Trier van, M. & Rietdijk, J.W. (2005) *Innoveren met RFID: op de golven van verbetering.* The Hague: Sdu Uitgevers. -147p.

Interviews

Elzinga, H. (Global Strategic Alliances & Programs Manager Identification Phillips) & Gijrath, J. (Director Business Development "Identification" EMEA & Relation Manager "Transportation" Phillips) 13 July 2006, held by Christian van 't Hof

Dr Jaap Henk Hoepman, Senior researcher in the Security of Systems group at the Institute for Computing and Information Sciences of the Radboud University Nijmegen 3 august 2006, held by Christian van ‘t Hof.

Meetings

6 June 2006, STOA Workshop RFID & Identity Management

26 June 2006, Think Tank RFID & Privacy (the Hague, the Netherlands)

18 September 2006, Think Tank RFID & Privacy (the Hague, the Netherlands)

Appendix: case studies

Case #4: METRO Group Future Store

Case ID	# 4, level 2
Title	METRO Group Future Store
Researcher	Jessica Cornelissen and Christian van 't Hof
Timing	April 2003 - present
Geography	Germany (Rheinberg)
Setting	Shopping
Environment	Grocery store (serving as a test site)
Technology	ICODE (high-frequency) and UCODE (ultra high-frequency), which are read-only passive chips. Tags are positioned on cartons, pallets and a few selected products. RFID readers in incoming and outgoing gates of the warehouse and in Smart Shelves. The maximum reading distance for product labels is approximately one meter operating at high frequency, whereas labels on cartons and pallets can be read up to six meters using ultra high frequency [1, 17]. "Mobile Assistant" handhelds for employees and the "Personal Shopping Assistants (PSA)" for customers communicate via a Wireless Local Area Network (WLAN) with the merchandise management system. [20] The De-Activator does not put the item-level tags in a dormant state, but it permanently disables the tag. In addition case-level tags are disabled at the information counter upon request by customers.
Maturity	Pilot
Function	Tracking and tracing of products
Owner	METRO Group Future Store Initiative [10]. This initiative is a joint platform of the Metro Group [11], Intel [12], IBM [13], T-Systems [14] and more than 60 other cooperating partners from the IT and consumer goods industries and the service sector
Maintainer	
Users	Suppliers, distribution centres, store employees, customers.
Other actors	- Intermec > supply of readers [18] - Philips Semiconductors (currently NXP) > supply of RFID chips [19] - Partners of the Metro Group Future Store Initiative involved in the RFID applications [15] - FoeBud e.V. > privacy group [8]
Case story	In the Future Store a combination of technologies is tested in a real setting. The purpose is to develop uniform standards and processes for warehouse management and the sales floor. A Metro spokesman said: " .. We want to see how [the technology assembled in an integrated environment, red.] will all work together and how customers will accept them." [1]. The Metro Group also operates the METRO Group RFID Innovation Centre, where the technique of RFID in several applications is pioneered in a laboratory setting [10]. RFID is most prevalent in supply chain management. Cartons and pallets are tagged and readers installed at the exits and entrances of distributions centres and the warehouse. Besides this, a number of selected items are individually tagged. This is done for two purposes. The first is for stock management using Smart Shelves. RFID readers incorporated in shelves scan the tags of individual products. Main functions are stock-control, checking for misplacement and quality control. The Smart Shelves also provide product information to the customer. The second purpose is customer-directed by giving customers the option to view or hear trailers of video and audio products. The tag in combination with the customer loyalty card serves as an 'age-key' by checking whether the customer has reached the appropriate age to see or hear the trailer. In order to disable the tags after a product is purchased, the store is equipped with a De-Activator [1, 6, 17]. According to the Future Store Initiative no personal customer data is stored on the RFID chips with regards to the supply chain management applications. This does not account for the tagging of items for test purposes. Customers can go to an information terminal to see which data is stored on the chips.[10].

	About a year after the opening of the Future Store, FoeBud protested against RFID in the store. Main issue was the coupling of information about customers' age on the RFID enabled loyalty cards to video and audio products, when using the in-store viewing service. According to Albrecht von Truchseß, a Metro spokesmen, this was done to meet German law on age restrictions. As a result of the protests, the retailer decided to recall the loyalty cards and restore barcode systems. However, the store says to be determined to keep RFID technology in the supply chain. "We remain totally committed to using RFID in the area of supply chain management," Mr Von Truchseß said. "A top priority is the use of this technology for tracking pallets and cases. And although we're still interested in testing the technology at the item level, this isn't a priority at the present." [3, 4, 5, 7, 9]. Besides the aforementioned matter on RFID loyalty cards, several other possible applications are being targeted by privacy advocates. Such as RFID enabled shopping carts that can track customer movements [2, 5]. Also, some claim a De-Activator was found ineffective [3]. In a response to our enquiry, Metro Future Store spokesman Daniel Kitsch claims there are no shopping cards tagged with RFID chips in the METRO Group Innovation Center, only a prototype shopping card equipped with a RFID reader (but no tag!) was shown. He also claims that: "At no point since its introduction in the METRO Group Future Store was the De-Activator ineffective. Parallel to the technological evolution in RFID tag and RFID chip technology the De-Activator has been constantly updated and has been able to actually disable the tags permanently the whole time. On occasions when regular maintenance services are undertaken, the De-Activator Terminal is clearly marked as "temporarily out of order" and customers are informed to refer to the information's desk for manual de-activation of the tag." [20] With regard to the customer loyalty card he stated: "Since 2004 there are no longer RFID chips in the EXTRA FUTURE CARD. Only for a very brief period of time in the early days of the METRO Group Future Store have only the purpose-built loyalty cards called EXTRA FUTURE CARD been equipped with a RFID chip. […] Customers who applied for an EXTRA FUTURE CARD was told orally that one of the new features of the card was a Smart Chip, as an additional storage medium, which would enable the preview application in the multimedia department of the store. In addition customers where invited to an introduction into the technological features of the METRO Group Future Store and received a brochure in which all technologies deployed in the store were explained, including Smart Chip/RFID technology." [20] "On the other hand, product-level RFID tags on media are only used to identify each of the units at the Information Terminal in order to allow the computer to start the relevant trailer. Should a DVD be age-restricted, the Information Terminal requires a further data input to verify that only person eligible to watch it are allowed to do so. In order to ensure that a person requesting a restricted movie trailer is eligible the Information Terminal needs to scan the barcode on the customer card. Because the Future Store generally does not sell media content restricted to people age 18 or older (the legislative term in German is: "Keine Jugendfreigabe", compare: http://www.spio.de/index.asp?SeitID=18 provides, visited September 13, 2006) the fact that a customer card has been issued to the customer is sufficient information to prove a person eligible. Customer cards can only be issued to people age 16 or older because the EXTRA FUTURE CARD used in the Future Store, is part of the PAYBACK loyalty card program in Germany (compare: http://www.payback.de/pb/ui/,19546,,?). It is important to stress that the Information Terminal in the multimedia department is not connected to the PAYBACK data management system and relies solely on the recognition of the PAYBACK number to deduce that the customer is eligible to see the restricted trailer. No personal data of the customer can be used for this authentication procedure."[20] Also "There is no personal data on any RFID chip used at METRO Group. Neither pallet-level nor case-level or item-level tags carry personal consumer data or can be relate to such data in a database. All tags carry an Electronic Product Code (EPC) which can only be related to product information and not to personal data. Because the item-level tags in the Future Store are only used for the limited purpose of operating and testing the "smart shelve" applications, tags are

	attached to the products in the backroom of the store. Accordingly, the tag's EPC is not scanned at the check out. It is therefore impossible to relate an individual product's EPC to any kind of purchasing information generate in the check out process. Nevertheless, after the point-of-sale METRO Group complies with privacy in the interest of its customers as a matter of course. In conjunction with partners from retailing and the consumer goods business METRO Group has voluntarily committed to using RFID responsibly (compare: http://www.future-store.org/servlet/PB/show/1008040/EPC_FSI%20english.jpg).[20] "There is no indication that the Future Store became unpopular neither in the public, nor among its customers. So far there have been more than 3.000 guided tours with overwhelmingly positive reactions from participants. The number of positive press articles by far exceeds the number of critical ones. In addition, METRO Group is engaged in regular dialogue with consumers, stakeholders and interested parties to discuss matters of consumer privacy and data protection. METRO Group also cooperates with scientific institutions to conduct consumer surveys (http://www.taucis.huberlin.de/_download/rfid.pdf#search=%22sarah%20spiekermann%20humbolt%20RFID%20METRO%20Future%20store%22) and research. Since opening the METRO Group Future Store in 2003 there is also an e-mail and telephone hotline through which we have yet to receive a single complaint. Every customer who applied for a – at the time new – EXTRA FUTURE CARD was told orally that one of the new features of the card is a Smart Chip." [20] "Only the age authentication application in the multimedia department, as the only application that was at the time operated with the Future Card RFID chip, was replaced by a system using the cards barcode, as described above. This was possible because at no time did the RFID tag in the Future Card carry any other information than the PAYBACK card number. Hence the same number which was at the time and still is today stored on the Future Card in its barcode, the magnetic strip as well as written visibly on its surface. No other application of RFID technology in the METRO Group Future Store has been changed or brought to a standstill." [20]
ID issue	The Future Store implemented RFID enabled loyalty cards. Pressure groups claimed the customers were not informed on this, triggering a public controversy. Metro therefore urged to withdraw some of its applications and re-issue bar coded loyalty cards. Since this event, there has been a close watch on the store by privacy groups. Metro claims there was no overall negative public response. Nevertheless, in much of the literature on RFID, this case is referred to as one of the bigger controversies in RFID and Identity Management.
Sources	1. ' Metro Opens 'Store of the Future''. In: RFID Journal, 28 April 2003 (http://www.rfidjournal.com/article/articleview/399/1/1/, visited 29 June 2006) 2. ' RFID for Your Shopping Cart'. In: RFID Journal, 1 July 2003 (http://www.rfidjournal.com/article/articleview/489/1/1/, visited 29 June 2006) 3. Best, J., ' Supermarket cans RFID trials in Germany'. 1 March 2004, (http://www.silicon.com/networks/lans/0,39024663,39118760,00.htm, visited 29 June 2006) 4. 'More on the Metro RFID consumer loyalty cards'. 2 March 2004 (http://www.rfidbuzz.com/news/2004/more_on_the_metro_rfid_consumer_loyalty_cards.html, visited 29 June 2006) 5. 'Metro zieht RFID-Karte zurück'. 27 February 2004 (http://www.heise.de/newsticker/meldung/45062, visited 29 June 2006) 6. Houtman, J., 'Online boodschappenlijst toegevoegd aan Future Store'. 3 May 2004 (http://www.emerce.nl/nieuws.jsp?id=279616, visited 29 June 2006) 7. Blau, J., 'Metro Store bows to pressure from anti-RFID activists' 1 March 2004 (http://www.infoworld.com/article/04/03/01/HNmetrostore_1.html, visited 29 June 2006) 8. http://www.foebud.org (visited, 29 June 2006) 9. Trier, M. van & J.W. Rietdijk (2005). Innoveren met RFID, op de golven van verbetering. Den Haag: SDU Uitgevers BV. 10. http://www.future-store.org (visited 22 August 2006) 11. http://metrogroup.de (visited 22 August 2006)

12. http://www.intel.com (visited 22 August 2006)
13. http://www.ibm.com (visited 22 August 2006)
14. http://www.tsystems.com (visited 22 August 2006)
15. http://www.future-store.org/servlet/PB/menu/1007073_l2_yno/index.html (visited 22 August 2006)
16. http://www.spychips.com/metro/overview.html (visited 22 August 2006)
17. 'A successful start for the future of retailing: welcome to the Future Store' (http://www.future-store.org/servlet/PB/show/1004095/off-Presse-Pressemat-FSI-Booklet-engl_05-01-10.pdf, visited 22 August 2006)
18. http://www.intermec.com (visited 30 August 2006)
19. http://www.semiconductors.philips.com (visited 30 August 2006)
20. E-mail correspondence with Daniel Kitscha from Metro Groups Corporate Communication. 29 September 2006.
21. http://www.futurestore.org/servlet/PB/menu/1007869_l2_yno/index.html, and
22. http://www.futurestore.org/servlet/PB/show/1011188/off-UeberdIni-Publik-Welcome-06-08-24.pdf

Case #6: Marks & Spencer Intelligent Label Project

Case ID	# 6 , level 1
Title	Marks & Spencer Intelligent Label Project
Researcher	Jessica Cornelissen
Timing	Spring 2006 - present
Geography	United Kingdom
Setting	Shopping
Environment	Clothing department of retail chain
Technology	Item level tagging with passive tags, using 868 MHz frequency. Tags are embedded in the 'Intelligent Label' on garments. Reading range is approximately half a meter. Tagging of trays and dollies in the distribution chain, using 13.56 MHz frequency. Readers can be either mobile (Mobile Store Reader (MSR)) or fixed (in the distribution centre) [1, 9, 12, 13]. The central database contains stock information of each specific item. This information is used for re-stocking and re-ordering [13].
Maturity	Pilot
Function	Tracking and Tracing of items
Owner	Marks & Spencer
Maintainer	Bt Group and Intellident ltd.
Users	Distributors, personnel in retail store
Other actors	- Consumers Against Supermarket Privacy Invasion and Numbering (C.A.S.P.I.A.N.) > privacy group [2] - Spy.org > privacy group [3] - BT Group > maintenance of database [4] - Intellident ltd > development of MSR [5] - Paxar corporation > production of labels [6] - EM Microelectronic > production microchips - Dewhirst > supply of goods [7]
Case story	Marks & Spencer has been testing RFID item-level tagging using the 'Intelligent Label' in several small-scaled pilots since 2003. In spring 2006 an extended trial in 53 stores was started. The basics of the technology remained the same as in the former pilots. However, the focus changed, from technique, to business to logistics. Also, the range of tagged items was broadened. The current system is in place to keep track of in-store inventory and ensure that a full range of sizes of any product is available to the customer [8]. In the earlier small-scaled pilots the Intelligent Label was attached to the product alongside the pricing label and designed to be cut off and thrown away after purchase. For pre-packed items, such as shirts, the tag was fixed on the bag [1, 11]. In the extended trial, the tags changed design. Instead of the RFID inlay being embedded in a separate label, it was incorporated into a single label that also carries a bar code and some text, including the note 'Intelligent Label for stock control use', advising customers [8, 10, 14]. The tags are read throughout the supply chain and in the store for stock taking. The tags are not used in the purchase-process [1]. During trial design and implementation, Marks and Spencer consulted privacy groups on possible privacy implications. These efforts led to positive reactions among sceptics. C.A.S.P.I.A.N. for instance acknowledged that Marks & Spencer has taken a socially responsible position. Despite these positive sentiments, C.A.S.P.I.A.N. denounced the trial in a press release, saying it does set a dangerous precedent by putting RFID tags in clothes [1].

	The retailer has chosen for minimal customer-directed use of the tag, avoiding privacy issues, and has taken efforts to inform his customers. In the brochure about the RFID tags, Marks and Spencer states that the label i) does not have a battery, ii) is harmless, iii) can be thrown away after purchase without losing the right to refund or returning and iv) will not be scanned at checkout. Instead, barcodes are scanned. This way, no link is made between the product and the customer, regardless the method of payment. [9, 11]. Contrary to the claim of Marks and Spencer that people have the freedom to throw away the label used in their trials, 'spy.org', another privacy group, states that the labels used in the earlier small-scales trials should be retained in order to maintain certain rights [3]. In a more recent publication on spy.org it is mentioned that this message has been removed on the newer labels [3].
ID issue	Using the RFID system only for the purpose(s) it has been implemented for, being cautious in expanding to further applications, could avoid controversy over privacy and identification. Informing consumers can be very important to prevent negative publicity and to increase understanding, even among sceptics.
Sources	1. 'U.K. Trial Addresses Privacy Issue'. In: RFID Journal, 23 October 2003 (http://www.rfidjournal.com/article/articleview/623/1/1, visited 26 June 2006) 2. http://www.nocards.org (visited 31 July 2006) 3. http://www.spy.org.uk (visited 1 August 2006) 4. http://www.btplc.com (visited 31 July 2006) 5. http://www.intellident.co.uk (visited 1 August 2006) 6. http://www.paxar.com/ (visited 31 July 2006) 7. http://64.233.183.104/search?q=cache:DeJ9T5WMfYQJ:www.dsionline.com/collateral/pdf/software/ss_Dewhirst.pdf+dewhirst+marks+spencer&hl=nl&gl=nl&ct=clnk&cd=4 (visited 31 July 2006) 8. 'Marks & Spencer to Extend Trial to 53 Stores'. In: RFID Journal, 18 February 2005 (http://www.rfidjournal.com/article/articleview/1412/1/1/, visited 28 June 2006) 9. 'Background to Marks & Spencer's business trial of RFID in its clothing supply chain'. (http://www2.marksandspencer.com/thecompany/mediacentre/pressreleases/2004/com2004-01-30-00.shtml, visited 26 June 2006) 10. Sullivan, L., 'Marks & Spencer Prepares To Expand Item-Level RFID Tagging', In: InformationWeek, 18 February 2005, (http://www.informationweek.com/story/showArticle.jhtml?articleID=60402017, visited 28 June 2006) 11. McCue, A., 'Marks & Spencer starts tracking tag trials: High Wycombe store to use RFID tags for men's clothes', 16 October 2003 (http://management.silicon.com/smedirector/0,39024679,10006439,00.htm, visited 28 June 2006) 12. 'EPC in Fashion at Marks & Spencer'. In: RFID Journal, 11 April 2003 (http://www.rfidjournal.com/article/view/377, visited 28 June 2006) 13. 'Marks and Spencer takes stock'. (www.btplc.com/innovation, visited 7 August 2006) 14. http://www.mandslibrary.com/(S(4kamypmlxhtres45gb0pyazc))/ThumbNails.aspx?SectionID=101&Place=Innovation&TopLev=Company&ID=450&ParentID=101&landingimage= (visited 1 August 2006)

Case #15: Air France-KLM Baggage handling

Case ID	# 15, level 1
Title	Air France-KLM Baggage handling
Researcher	Jessica
Timing	July 2006 – March 2007
Geography	The Netherlands (Amsterdam) and France (Paris)
Setting	Border crossing
Environment	Luggage handling on flights
Technology	Passive UHF tags 'Monaco' by Impinj, compliant with ISO 18000 6C standard. Chips are read-write/re-write and equipped with 64 bits of memory beyond the standard 96-bit electronic product code. The baggage labels and the RFID solution are developed by IER.
Maturity	Pilot
Function	Tagging and tracing of products
Owner	Air France-KLM [1]
Maintainer	Amsterdam Schiphol Airport [2]
Users	Travellers and parties involved in luggage handling at both airports
Other actors	- International Air Transport Association (IATA) > coordinating body on RFID applications in airline industry [3] - Impinj > production of microchips [9] - IER > development of RFID solution [10] - IATA member airlines []
Case story	In 2004 the IATA launched a programme to test and build a business case for the use of RFID for baggage management. In November 2005 the organisation introduced a global standard for RFID baggage tags, named RP1740C. Air France-KLM functions as a pilot airline to further test RFID in baggage handling and this test is part of the IATA programme [5, 6]. KLM/ Air France performs the trial with RFID tags to label and track baggage on flights between Paris-Charles de Gaulle and Amsterdam Schiphol Airport. Later in 2006 more drop-off points in Amsterdam Schiphol Airport will be using RFID labels. Also, flights between Paris-Charles de Gaule and Tokyo Narita airport will take part in the trial at a later stage [4]. The goal of the pilot is to improve the baggage handling process. By implementing RFID labels more reading points are possible, because of automated reads and a higher read rate than bar codes. Thus, bags can be sorted and loaded faster than bar code systems and the number of mishandled bags and associated costs is reduced [5, 6]. A visitor of a forum on ICT development posed his doubt about the safety of the system. He refers to the alleged possibility to undermine the functioning of the database by deploying chips with false ID-number [7]. However, another visitor of the forum refuted this possibility. He also mentioned that from a privacy perspective the situation is not different from the older bar code system, but that the fact that RFID can be read without line of sight can be alarming. He writes: 'In my view, the acceptance of RFID technology forces us to develop methods and techniques that prevent the gathering and sharing of information 'behind peoples backs' [8].
ID issue	It seems as though public opinion on a new technology is susceptible to irrelevant or false claims about privacy. The party running the pilot might not foresee any privacy concerns, but these concerns could rise. Also the fact that someone's property is tagged, could make it more prone to concern from the public.
Sources	1. http://www.klm.com, visited 30 August 2006 2. http://www.schipholairport.com, visited 30 August 2006 3. http://www.iata.org, visited 30 August 2006 4. 'Air France and KLM test radio frequency identification tags for baggage handling and tracking management.' 3 July 2006 (http://www.klm.com/travel/corporate_en/press_room/press_releases/index.htm?id=39399,

	visited 14 July 2006).1. 'KLM en Air France rusten bagage uit met rfid-chip', 3 July 2006 (http://www.webwereld.nl/articles/41839/klm-en-air-france-rusten-bagage-uit-met-rfid-chip.html, visited 4 July 2006). 5. 'IATA Introduces Global Standard for Baggage Tags', 20 November 2005 (http://www.rfidinternational.com/news.php?action=full_news&NewsID=103, visited 5 July 2006) 6. Collins, J., 'Air France-KLM Embarks on RFID Luggage-Tag Trial.' In: RFID Journal, 18 August 2006 (http://www.rfidjournal.com/article/articleview/2600/1/1/, visited 4 September 2006) 7. Comment by 'Thyxx' on 3 July 2006 (http://www.webwereld.nl/comments/41839/klm-en-air-france-rusten-bagage-uit-met-rfid-chip.html, visited 4 September 2006) 8. Comment by 'Xtian' on 3 July 2006 (http://www.webwereld.nl/comments/41839/klm-en-air-france-rusten-bagage-uit-met-rfid-chip.html, visited 4 September 2006) 9. http://www.impinj.com/page.cfm?ID=Chips (visited 4 September 2006) 10. http://www.ier.fr/htmleng/acceng/accueileng_estore.html (visited 4 September 2006) 11. http://www.iata.org/membership/airline_members.htm (visited 6 September 2006)

Case #18: Baja VIP Chip

Case ID	# 18, level 3
Title	Baja VIP Chip
Researcher	Jessica

Timing	2004 – present [1, 2]
Geography	Spain (Barcelona) and The Netherlands (Rotterdam)
Setting	Fun
Environment	Night Club

Technology	Implantable read-only passive RFID tags with 16 digit ID-number by VeriChip Corporation. The chip can be implanted subcutaneous with a syringe. The database contains a carrier's information and is linked to an electronic payment system. [3, 4,11]
Maturity	Operational
Function	Identification, access and payment
Owner	Baja Beach Club
Maintainer	Baja Beach Club
Users	- VIP guests of the night club - Personnel and management of the night club
Other actors	– VeriChip Corporation > provider of – The No VeriChip Inside Movement > privacy and digital civil rights group [7] – The Resistance Manifesto > religious group [8] – Bits of Freedom > digital civil rights group [9] – U.S. Food and Drug Administration > public health institution [17]
Case story	The nightclub has a VIP lounge that is only accessible for VIP guests. These guests are distinguished from regular guests by an implanted chip. Currently there are approximately 70 people that carry the chip in The Netherlands, of which more than 80% are male. Mr. Van Galen explains that the number of VIP's will not be increased, because it has to remain an exclusive thing. The VIP area is separate from the rest of the club and has its own bar and personnel. A VIP Chip carrier is allowed to bring one or two friends to the area [6, 10, 12, 15]. Upon implanting the chip one has to sign a statement of free will, also containing an acknowledgement that the chip and the information will remain property of the nightclub. A carrier can decide to have the chip removed any time and without former notice to the nightclub [15]. VIP Chip carriers enter the club through the main entrance. Upon entering, a carrier does not have to show an identification nor does he or she has to pay an entrance fee. Personnel scan the implanted chip with readers provided by VeriChip, after which the details of the carrier are presented on a computer at the entrance. On the screen of the reader, only the ID-number of the chip is displayed. Details displayed on the computer are ID-number of the chip, name and photo of the carrier, balance on the chip and transaction history. The transaction history consists of transaction amount, time of transaction and bartender running the transaction. The scanners that are used are handheld and only operated in the VIP lounge and at the entrance. The computers too are only present in the VIP lounge and at the entrance [15]. The database is property of the nightclub; no third parties have access to the information. The technology is an 'in-house system', where no information goes outside the club and no personal information is taken [13, 15]. In an interview, the director of the Baja Beach Club Barcelona Conrad Chase says the chip was introduced for two reasons. Firstly, for the image of the nightclub, they wanted to offer their guests an original item. Secondly, to benefit from the latest most advanced technology, something that could offer convenience for both the nightclub as well as the carriers [12]. According to Mr. Van Galen, the VIP Chip was supposed to support the VIP treatment, but should not be or become an issue on its own; the nightclub's main concern is operating a business. He recognises the multiple opportunities the technology has, but is cautious about expanding the applications of the chip. This

	has two reasons; one is the business priority. The other is the fact that society and media tend to explain the technology in a negative manner. Consequently Mr. Van Galen is very much aware that opinions on the technology can change easily from positive to negative and that this can harm the nightclub's image [15]. The director of the Baja Beach Club in Barcelona has a different opinion on this. Chase says 'the objective of this technology is to bring an ID system to a global level that will destroy the need to carry ID documents and credit cards. The VeriChip that we implant in the Baja will not only be for the Baja, but is also useful for whatever other enterprise that makes use of this technology'. In addition, a Rotterdam club promoter shares this view: 'If the government offered this as a choice, saying you can put your ID card, your social security card and your credit card away and just have this, I'd sign immediately. I would not have to carry around my wallet. If I need to go to hospital, even if I am unconscious, they could just scan and get my records'. Some regulars of the nightclub are probably also in favour of expanding the applications. One of the VIP guests of the Baja Beach Club Rotterdam, Steve van Soest says the following: 'The main benefit is that you can go out without having to carry a wallet, which can get easily lost in a night club.' […] 'It would be great if this catches on and you could put all your personal details and medical records on it. If I was involved in an accident, doctors could simply scan me and find out my blood group and any allergies.' Other sources indicate that this person might also be a club spokesperson, so his opinion might be skewed because of this. [12, 13, 14, 16]. Mr. Van Galen thinks the carriers regard the chip as a special gadget that supports the VIP treatment in a positive way. Carriers value the fact that they do not have to show identification nor have to handle money. This adds up to the feeling of being an appreciated guest of the club. He also thinks this might be the reason why more men than women carry the chip; 'women want to be invited to the VIP area, whereas men want to invite women' [15]. The club uses the system as an informal loyalty system, however the technology is not a key-instrument in this; it could also be done without, based on personal experiences with guests. Regulars and 'big-spenders' get offers like first options to limited tickets, invitations to special nights and Mr. Van Galen even mentioned offering a airplane ticket to a Spanish guest. Guests regard this loyalty scheme as positive, according to our respondent [15]. Development the night club is looking into are the following: 1. Using a credit system Mr. Van Galen thinks using a credit system, which involves the necessary linking the ID of the chip directly to a bank account or credit card, has both advantages and disadvantages. An advantage could be that a guest would never have to hand over any cash or bankcard. This could enhance the feeling of exclusiveness. A disadvantage could be that it does not 'protect' a guest from spending more than intended, since there is no maximum amount to spend. Furthermore, it involves issues of privacy and safety. 2. Chipping personnel Currently, personnel of the nightclub carry tokens with chips in them. This way they can enter through a personnel entrance. However, the token could be transferred to another person. The implant could have a big advantage there, since it cannot be transferred nor lost be the carrier. Mr. Van Galen says not to have the intention to use it as time-registration. 3. Expanding to more clubs in Europe and linking VIP guests European-wide Mr. Van Galen is in favour of the application expanding to other nightclubs. He envisions a 'chippers-community' in which VIP Chip carriers from different nightclubs can meet (in person or virtual) and in which they can use their status in associated clubs. 4. A more 'aesthetic' way of scanning guests Mr. Van Galen is not satisfied with the scanning process as it is right now. The scanner needs to be put very close to the chip and thus to the carriers' arm. Reading chips from a greater distance would be a solution, but it is impossible to enlarge the chip antenna. Getting bigger readers would be an option, but it is unclear whether this would work in practice [15].
ID issue	Most controversy on this RFID application is about implanting a chip in the human body. Main issue is the violating of one's personal integrity. Also, some belief it is 'the mark of the beast'. On the other hand, implanting the VIP Chip is done out of free will and having such an implant is not a

	necessity. Information on 'clubbing' and drinking behaviour will be accessible to the nightclub. It is up to the potential carrier to decide whether he or she finds this acceptable.
Sources	1. 'Applications Continue to Grow for Applied Digital Solutions' VeriPay Baja Beach Club in Barcelona, Spain Employs RFID Technology for Cashless Payment System' 05 April 2004 (http://www.findarticles.com/p/articles/mi_m0EIN/is_2004_April_5/ai_114927021, visited 20 June 2006). 2. 'Een onderhuids dranktegoed' In: Algemeen Dagblad, 01 October 2004. 3. http://www.verichipcorp.com (visited 20 June 2006) 4. 'Implantable RFID Tags' (http://www.verichipcorp.com/content/company/verichip#implantable, visited 20 June 2006) 5. 'Bedrijf wil onderhuidse identificatiechip beproeven.' In: Automatisering Gids Webeditie, 28 February 2002 6. Slingerland, C.S. 'Presentatie Baja Vip Chip', 24 May 2006. Rotterdam, Emerce. 7. http://noverichipinside.com (visited 21 June 2006) 8. http://www.theresistancemanifesto.com (visited 21 June 2006) 9. http://www.bof.nl (visited 21 June 2006) 10. Hemment, D., 'Interview with Conrad Chase.' 19 June 2004. (http://www.drewhemment.com/2006/interview_with_conrad_chase.html, visited 21 June 2006) 11. http://en.wikipedia.org/wiki/Verichip (visited 20 June 2006) 12. 'Conrad Chase, Director of Baja Beach Club's Interview with the EFE News Agency about the VIP VeriChip' (http://www.bajabeach.es, visited 20 June 2006) 13. Hemment, D., 'Last Night An Arphid Saved My Life'. (http://www.drewhemment.com/2006/last_night_an_arphid_saved_my_life.html, visited 20 June 2006) 14. Martin, L., This chip makes sure you always buy your round.' In: The Observer, 16 January 2005 15. Personal communication with Mr. Van Galen, Managing Director of the Baja Beach Club Rotterdam, 4 August 2006 16. 'I've got you under my skin.' In: The Guardian, 10 June 2004. 17. http://www.fda.gov (visited 29 August 2006)

Case #19: FIFA World Cup Germany Tickets

Case ID	# 19, level 1
Title	FIFA World Cup Germany Tickets
Researcher	Jessica Cornelissen
Timing	December 2005 – July 2006
Geography	Germany
Setting	Leisure
Environment	Football stadium
Technology	Passive chips incorporated in the access-ticket for the event, chips are supplied by Phillips (MiFARE Ultralight, ISO 14443, Ultra-high frequency). The software is from CTS Eventim
Costs	0,10 per ticket (total of 3,2 million tickets sold) [5]
Maturity	Operational
Owner	FIFA World Cup Ticketing Centre
Maintainer	German Football Association (DFB), system provider CTS Eventim
Users	- Visitors to world cup 2006 matches - Stadiums participating in the 2006 World Cup
Other actors	- FoeBuD [6] > Privacy group - Datenschutz Zentrum > Data Protection Centre [7] - Bündnis Aktiver Fußball-Fans (BAFF) > Alliance of active football fans [8]
Case story	The technology is applied to combat counterfeiting and to ensure only those with legitimate tickets can get in. This way it also serves as 'hooligan prevention/monitoring'. The chips will only be scanned at the entrance of the stadium. Inside the stadium there will be no scanners [11, 12]. On applying for a ticket one has to provide personal information: name, address, nationality, sex, date of birth, passport number, e-mail address (optional), telephone number (optional) and, possible, also the club you are supporting. This information is stored in a database and linked to the ID-number on the chip [6, 10]. Other applications, like contactless payment, were explored but rejected because of expected problems over privacy [11]. Germany's football authorities have been accused of 'Big Brother tactics'. Privacy groups claim that the ticketing centre requests for irrelevant information and that it doesn't make clear what is done with the information. Furthermore, they claim that opt-in procedures on on-line sales questionnaires were not clear. [6, 7, 9]. FoeBuD states that the ticket are being sold under false pretexts, like security reasons, and that it is unfair to insert this kind of technology in an item that much wanted by fans. "What could be nicer: A top-event with millions of enthusiastic people who would do just about anything for their most beloved hobby. Add to this a September 11 heralding no end of "threat by terrorism", and you have all the justification you need for just about any measure to cut down on freedom rights as long as there is a sticker on it saying "security". And should the World Cup go past without any assaults you have every justification to afterwards call the whole "security-concept" a success, RFID in the tickets and all, and silence all the critics with a hearty salute: "Hey, all of you conspiracy theorists, hundreds of thousands of soccer fans didn't have any problems with RFID!" " [6]. Also, the German Data Protection Centre states on their website that supervision and security are two different things. Therefore, introducing technologies under the pretext of enhanced security cannot be done just like that [7]. Privacy groups have a lot of concern regarding the protection of personal data. However, some of the assumption they do are false or far-fetched. The FIFA state on the website that personal data will be processed in compliance with the Data Protection Legislation applicable and that data will be shared to third parties (like security agencies, stadium operators and shipping providers) only if necessary [10].

ID issue	Implementing RFID technology in a place where users have no choice to use it or not, brings about controversy. Also, because policies on data sharing and protection remained unclear for a long period, as well as the actual occasions a ticket would be read, privacy groups could cause a lot of negative publicity. In addition, the widespread and thorough implementation of the technology makes it quite likely that it will be maintained at the stadiums and used on regular matches after the World Cup event. Sceptics think the World Cup serves as a test to see how the technology works out in practice and as a mean of justification afterwards.
Sources	5. Libbenga, J., 'World Cup Tickets will contain RFID chips.' 04 April 2005. (http://www.theregister.co.uk/2005/04/04/world_cup_rfid/, visited 26 July 2006) 6. http://www.foebud.org (visited 26 July 2006) 7. http://www.datenschutzzentrum.de (visited 26 July 2006) 8. http://aktive-fans.de (visited 26 July 2006) 9. Ermert, M., 'World Cup 2006 'abused for mega-surveillance project'.' 08 February 2005. (http://www.theregister.co.uk/2005/02/08/world_cup_2006_big_brother_charges/, visited 26 July) 10. http://fifaworldcup.yahoo.com/06/en/tickets/overview.html (visited 09 July 2006) 11. Best, J., '3,2 million World Cup tickets RFID chipped.' (http://networks.silicon.com/lans/0,39024663,39159715,00.htm, visited 07 July 2006) 12. 'Philips ticket technology opens the doors of the FIFA World Cup', 14 June 2006. (http://www.semiconductors.philips.com/news/content/file_1245.html, visited 28 August 2006)

Case #23: the European Biometric Passport

Case ID	23, level 3
Title	Passport
Researcher	Sil Wijma
Timing	2006
Geography	Europe
Environment	Border control, identification
Technology	Passport with RFID tag, 13,56 MHz, different readers.
Maturity	Pilot
Function	Identification
Owner	Different European countries
Maintainer	International Civil Aviation Organization (ICAO)
Users	Citizens
Other actors	Different governments, different manufacturers (Philips, Oberthur Card Systems, Setec, etc.), European Union and different consumer organisations such as Bits of Freedom (BOF).
Case story	RFID passport in Europe European countries are introducing RFID-tags in passports to improve security of the passports. This is partly because of demands from the USA to store biometric data on the passport and because of the wish to improve the security of the passports. Nations participating in the U.S. Visa Waiver Program have to implement new passports with biometric features that support facial recognition. Biometric data such as a digital photo is therefore stored on the passport-chip. The main target of this is to prevent look alike fraud. The International Civil Aviation Organization (ICAO) has developed standards for the use of biometric data in passports [31]. The ICAO is busy with the possible use of biometric data since 1997 [30]. The ICAO decided in May 2003 to use facial recognition in travel documents [30]. The European Union followed in September 2003 with the decision to use a photograph and two fingerprints [30]. The technical specifications were determined on the 28th of February 2005 [35]. At first only digital photographs will be saved on the chip inside the passports. Later additional biometric data can be added, such as fingerprints, DNA-profiles and iris-scans. Adding fingerprints was more difficult then first thought and therefore all European Countries have to store fingerprints on the chip inside the passports from the 28th of June 2009 [23]. There are different uses of the biometric passports: verification (one to one), identification (one to many) and screening [27]. The European Union first wanted biometric passports to be introduced in January 2005, but delays occurred. The first country to use the biometric passports was Belgium that issues the passports since November 2004 [different chip?]. Germany followed in November 2005 [20]. One of the ways the data on a passport is secured is 'basic access control' (BAC). This is a way to prevent skimming. Some information of the passport and its holder is summarized in a Machine Readable Zone (MRZ). The MRZ consists of two lines of optically readable text with (among other data) the name of the holder and passport number. A reader has to read the MRZ before being able to retrieve data from the chip inside the passport [26]. This means a passport has to be opened to be read. Basic access control is important although it is then questionable why a contact less chip is needed. Researchers also found out that some information on the passport chip is retrievable without access to the MRZ [26]. Because of this there are ideas to use metal to prevent any reader from accessing the chip in the passports. The USA for example uses metal fibres in the front cover in order to prevent unauthorised reading [48]. When access to the chip is granted information will be exchanged. This information exchange between chip and reader is secured (secure messaging). This means the information is encrypted and uses a message authentication code (MAC) [26]. Further the integrity of the data on the chip is checked with Passive Authentication (PA) and Active Authentication (AA) further prevents cloning. But there are reports that the passports can be cloned, although it was not possible to alter

	the data on the chip [10, 48]. The European Union developed an extra security measure known as 'Extended Access Control'. This measure increases the security of the passport but it is unclear whether this is sufficient. Extended Access Control consists of two phases, Chip Authentication followed by Terminal Authentication. CA uses Document Verifier (DV) Certificates [26]. Researchers showed that the encryption used on the passport could easily be cracked [13, 25]. Also eavesdropping is easier than earlier thought. The signals used to communicate between a passport chip and a reader can be read from more then 9 meters [28] while in laboratories 50 meters is possible [6]. But according to a governmental website the Dutch passport was not cracked (because it was not issued yet, only a preliminary version was used) [43]. The chips in the passports use an anti-collision identifier (sort of a identification number). This should not be fixed because it makes tracking of people possible, apart from bombs that are triggered by the identification number [26, 10, 56]. But even without a fixed number there is some information revealed, for example the nationality of the holder of a passport. The nationality of the holder can therefore be used to trigger a bomb [56]. For Identity Management flexibility is needed for different occasions and settings. The passport on the other hand has a rigid format. Therefore all information is revealed, even if only the age of a person has to be verified [26]. There are also questions concerning the use of central databases. Hereby the fear is that later new functions for the use of the data will be invented. This is called 'function creep', i.e. data can be used to identify people with fingerprints or video systems can (automatically) identify people. The security of the central database is of coarse also very important. Biometrical data can contain different sorts of information. A photograph for example can tell a lot about a persons religion. All sorts of biometrical data like fingerprints, photographs and retina scans can contain medical information [1]. Apart from that there might be other problems because the large-scale use of biometry is untested [26]. Further there are problems with the use of the gathered biometric data. Digital photographs can be placed on chips but identification of persons by this photo is not flawless, especially with children and elderly [37]. A newspaper says the fault margin is 25 percent [29]. For fingerprints this is 2 to 3 percent [59], apart from the easy duplication of fingerprints [6]. European Data Protection Supervisor (EDPS) also warned against the use of multiple, connected databases because biometric data is not as reliable as often thought [23]. It is suggested that the European Union wants to store biometric data in large databases [23]. Only 5 of the 25 member states of the European Union (Austria, Belgium, Denmark, France, Germany, Sweden and the Netherlands) started issuing the new biometric passports on time (28th August 2006) [57]. A further five countries have said they would be ready a week later and a few others may be ready or close to readiness without having informed the commission about it [57]. Italy RFID-passport is popular [Philips contact]. No central database to be used [15]. Netherlands The Netherlands has been busy renewing the passports for some time now. A New Generation Travel documents (Nieuwe Generatie Reisdocumenten, NGR) was introduced in October 2004 [34]. Later the Netherlands followed the new regulation from the European Union in the use of biometric data. The Netherlands introduced the biometric RFID passport in august 2006. For now it only contains a digital photograph, later digital fingerprints will be added. In 1998 there was already discussion about the use of biometric data in passports [29, 30]. The Netherlands further considers using a central database to store the collected (biometric) data [5, 35, 40]. Until now there are decentralised databases [40]. The idea is to continue to use the decentralised databases – also for the digital photographs – until the introduction of the fingerprints in the passport; then a central database is to

	be used. But this has not yet been discussed in the parliament. At the moment an alteration of the law is prepared which will be discussed at the end of 2006 [35, 40]. There is already protest against this, some say that at first the passport was to prevent look-a-like fraud but now the passport is to be a broadly applicable control and tracking mechanism [2]. Other warn for function creep whereby the technological possibilities of a central database will eventually be used, despite of privacy implications [4, 5]. There are two main arguments to install a central database; to prevent counterfeit and to fight terrorism [35]. The idea is to use a central database that can be accessed over the internet in order to check the legitimacy of passports. In this way it is possible to verify the data on the document itself, the data on the chip in the passport and the data in the central database which makes it more difficult to change an existing passport [35]. An article in a Dutch newspaper stated that a central database is already constructed although the parliament has not yet decided whether such a database is wanted [4, 5]. A minister reacts to this by saying that a database is not yet being constructed; the ministry only examines the possibilities [40]. The Dutch 'College Bescherming Persoongegevens' (CBP) is opposed to a central database because people have to prove their identity in many different occasions, which may cause coupling of different databases [59]. A research in 2002 showed that facial recognition to prevent look alike fraud is insufficient. Fingerprints and iris scans are much better usable for this purpose, although the use of iris scans is more difficult to use and more expensive because of a patent on the technology. Therefore fingerprints will be used [30]. The Netherlands further held a pilot with RFID-tags in passports between August 2004 and February 2005. Hereby a facial scan and fingerprints were stored on the passports chips of 14.504 participants [37]. The research covering this pilot only looked at the practical use of the biometric data and not at other aspects like privacy issues [37]. The introduction of the new passport in the Netherlands has been a bit chaotic. The media soon came with stories that the photograph of many people was rejected at the municipal- or town halls were they applied for a new passport [54, 55]. Later it appeared that a smile is not forbidden although only a slight smile is accepted [52]. The rules were apparently not clear enough for all governmental organisations [52]. Apart from unclear rules still 1,5 percent of the photographs was rejected by the manufacturer after one week of issuing the new passports [52]. There have also been a few passports with an unrecognisable photograph while the supplied photograph was meeting the demands [55]. And some complain about the demands for the photograph because it almost impossible to take a photograph of a baby with its mouth shut and facing the camera [53]. There are also reports that passport have been issued without a digital scan because the provided photograph was not good enough [53, 54, 55]. People with such a passport might encounter problems when travelling [54]. There have been different forms of protest against the new RFID passport. Some started a petition in order to prevent the introduction [49]. Others even give the advice to put the passport in the microwave in order to destroy the RFID-chip [58]. And some have questions about tracking and tracing, especially about the possible coupling of old cases with fingerprints [51] There is also fear for control in general [50]. This is partly because the chip can be read from some distance as mentioned above [6]. Some therefore suggest to put aluminium foil around the passport [60]. Germany Germany introduced the biometric RFID passport (called ePass) in November 2005 [1]. In March 2007 fingerprints will also be stored on the chip [44].. Later additional biometric data can be added, like an iris scan and some genetic information. German biometric passports are produced by the German Federal Printing Office (Bundesdruckerei), using chips supplied by Philips and Infineon Technologies [20]. Data stored on the German e-passport chips will be encrypted using the RSA public-key cryptosystem [20]. In Germany the idea has been put forward to sell personal data to cover the high costs of the passport [18]. These costs could rise to about €270 when more biometric data is stored in 2008 [22].

	The price of the new passport is €59 which is a lot more than the previous €23 [20]. According to one source there are two reasons why RFID chips are used in the passports; contact points in traditional chip cards are not designed for 10 years of use and because passports simple don't fit in current chip-card readers [21]. These arguments are not convincing since a reader has to be develop anyway and the lifetime of RFID chips is questionable as well. United Kingdom Issuing started on the 21st of April 2006. In 2004 there has been a trial from the UK Passport Service from April to December in which more than 10.000 persons participated [1]. The UK does not use the word RFID, instead use 'contacless' or 'proximity', probably because of a negative connotation attached to the word RFID [7]. There has been a report that the data collected for the passport was to be sold to keep the price down [45]. This is like the idea that was put up in Germany [18]. Minister Tony McNulty said banks would be able to verify card details against a database for a fee, but he said the information would not be sold [46]. Sweden Issuing started in October 2005 Supplier: smart card and security printing company Setec (recently acquired by Gemplus) [12]. Denmark Introduced on the 1st of August 2006 Supplier: smart card and security printing company Setec (recently acquired by Gemplus) [12]. Austria Introduction date is the 16th of June 2006 Belgium Issued since November 2004 [12]. The Belgian e-passport is manufactured by Oberthur Card Systems [12]. For now the Belgium passport contains a digital photograph, personal information and autograph [23]. Fingerprints will be added later. According to a source the passport chip of two different persons had accidentally been exchanged. One person found this out when her passport was scanned on a camping site in Spain [9].
ID issue	Researchers showed that the encryption used on the passport could easily be cracked [13, 25]. Also eavesdropping is easier than earlier thought. The signals used to communicate between a passport chip and a reader can be read from more then 9 meters [28] while in laboratories 50 meters is possible [6]. Biometrical data can contain different sorts of information. A photograph for example can tell a lot about a persons religion. All sorts of biometrical data like fingerprints, photographs and retina scans can contain medical information [1]. Apart from that there might be other problems because the large-scale use of biometry is untested [26]. Further there are problems with the use of the gathered biometric data. Digital photographs can be placed on chips but identification of persons by this photo is not flawless, especially with children and elderly [37].
Sources	01. Dessimoz, D. & J. Richiardi (2006) Multimodal biometrics for identity documents (http://www.europeanbiometrics.info/images/resources/90_264_file.pdf, visited 28 July 2006). 02. Mom, P. (2006). 'Groeiend verzet tegen paspoortbiometrie'. In: Automatisering Gids, nr. 5, 2006, Den Haag. 03. 'Kamer eist stop opslag biometrie'. In: Nieuwsbrief Bits of Freedom, nr. 4.5, 6 March 2006 (http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_5.html, visited 29 June 2006). 04. 'Kamer eist stop op opslag gelaatsscans en vingerafdrukken'. In: De Volkskrant, 25 February 2006 (http://www.volkskrant.nl/den_haag/article231026.ece (visited 5 July 2006). 05. 'De wereld van Orwell lijkt bijna onvermijdelijk' In: De Volkskrant, 25 February 2006

(http://www.volkskrant.nl/binnenland/article231020.ece (visited 5 July 2006).
06. '2006: het jaar van het biometrisch paspoort', 6 January 2006 (http://www.netkwesties.nl/editie138/artikel1.html, visited 5 July 2006).
07. ''RFID tag' - the rude words ID card ministers won't say: Lengthy descriptions of duck, but no d-word', 30 January 2006 (http://www.theregister.co.uk/2006/01/30/burnham_rfid_evasions/, visited 6 July 2006).
08. EBP (2006) Biometrics in Europe: Trend report. Brussels: European Biometrics Portal (http://www.europeanbiometrics.info/images/resources/112_165_file.pdf, visited 28 July 2006).
09. 'Chips op Belgische identiteitskaarten verwisseld', 30 August 2006 (http://www.clubmetro.nl/index.php?actie=nieuws&c=1&id=64223, visited 31 August 2006).
10. 'Rfid-paspoort vol met beveiligingslekken', 3 August 2006 (http://www.webwereld.nl/articles/42291/rfid-paspoort-vol-met-beveiligingslekken.html, visited 4 August 2006).
11. Kc, G.S. & P.A. Karger (2005) Preventing attacks on MRTDs, http://eprint.iacr.org/2005/404.pdf (visited 25-07-06).
12. 'SE: Biometric passports introduced in Sweden and Norway', 07 October 2005 (http://europa.eu.int/idabc/en/document/4792/194, visited 25 July 2006).
13. 'Nederlands paspoort al gekraakt voordat het uit is', 30 January 2006 (http://www.security.nl/article/12842/1/Nederlands_paspoort_al_gekraakt_voordat_het_uit_is.html, visited 05-07-06).
14. 'Paspoort met RFID-chip gepresenteerd: Aan de buitenkant nauwelijks anders', 25 April 2006 (http://www.zdnet.nl/news.cfm?id=55905 (14-07-06).
15. 'Italy: Decree to implement electronic passports containing biometric data: biometric data collected 'will not be stored in databases", 8 February 2006 (http://www.statewatch.org/news/2006/feb/08italy-biometric-passports.htm, visitied 17 July 2006).
16. 'ID cards an interference', 27 January 2006 (http://www.mirror.co.uk/news/voiceofthemirror/tm_objectid=16633371%26method=full%26siteid=94762-name_page.html, visited 10 June 2006).
17. 'Europa wil uitstel invoering biometrisch paspoort: Gros lidstaten haalt Amerikaanse deadline niet', 5 April 2005 (http://www.zdnet.nl/news.cfm?id=44553, visited 10 July 2006).
18. 'Käuflich: Personalausweis-Daten auf Bestellung', 2 February 2006 (http://www.chip.de/news/c1_news_18539262.html, visited 6 July 2006).
19. 'Gesellschaft für Informatik lehnt Verkauf von Personalausweisdaten durch Regierung ab: Bürger werden informationell und gesundheitlich durchleuchtet', 11 April 2006 (http://de.internet.com/index.php?id=2042438&section=Security, 6 July 2006).
20. 'DE: Germany to phase-in biometric passports from November 2005', 7 October 2005 (http://europa.eu.int/idabc/en/document/4792/194, visited 25 July 2006).
21. 'Germany plans passports with biometric data in November', 2 June 2005 (http://mathaba.net/x.htm?http://mathaba.net/0_index.shtml?x=234451, visited 6 July 2006).
22. 'German group opposes sale of biometric passport data: Government planned to fund changeover with sale of personal info', 11 April 2006 (http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110413, visited 6 July 2006).
23. 'Europese Commissie legt regels vast voor vingerafdrukken op paspoort', 29 June 2006 (http://ipsnews.be/news.php?idnews=7340, visited 10 June 2007).
24. 'Stille Post im digitalen Dorf', 4 February 2006 (http://www.heise.de/tp/r4/artikel/21/21937/1.html, visited 6 July 2006).
25. 'E-passports without the big picture', Hoepman & Jacobs, 20 February 2006 (http://www.egovmonitor.com/node/4716, 17 July 2006).
26. Hoepman et al. Crossing Borders: Security and Privacy Issues of the European e-Passport. Nijmegen: Radboud University, unpublished.
27. IPTS (2005). Biometrics at the Frontiers: Assessing the Impact on Society, February 2005, European Commission; Joint Research Centre (http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/iptsBiometics_FullReport_eur21585en.pdf, visited 11 July 2006).
28. Juels, A., D. Molnar & D. Wagner (2005). Security and privacy issues in E-passports. Securecomm 2005 (http://eprint.iacr.org/2005/095.pdf, 25 July 2006).
29. Kamerstuk 2003-2004, 25764, nr. 005.
30. Kamerstuk 2003-2004, 25764, nr. 022.

31. Kamerstuk 2003-2004, 25764, nr. 022, Bijlage 1.
32. Kamerstuk 2003-2004, 25764, nr. 022, Bijlage 2.
33. Kamerstuk 2003-2004, 25764, nr. 022, Bijlage 3.
34. Kamerstuk 2004-2005, 25764, nr. 024.
35. Kamerstuk 2004-2005, 25764, nr. 026.
36. Kamerstuk 2004-2005, 25764, nr. 027.
37. Kamerstuk 2004-2005, 25764, nr. 027, Bijlage 1, Evaluatierapport.
38. Kamerstuk 2004-2005, 23490, nr. 350.
39. Kamerstuk 2005-2006, 25764, nr. 028.
40. Kamerstuk 2005-2006, 25764, nr. 029.
41. Jacobs, B. & R.W Schreur (2005). Security review of the biometric passport. VVSS 24 November 2005 (http://www.cs.ru.nl/~bart/TALKS/jacobs-vvss05.pdf, visited 28 July 2006).
42. KST 2293
43. http://www.bprbzk.nl/ (visited 31 July 2006).
44. http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Themen/Informationsgesellschaft/DatenundFakten/Biometrie.html (visited 31 July 2006).
45. 'Ministers plan to sell your ID card details to raise cash', The Independent, 26 June 2005 (http://www.mkno2id.org/article1.htm, visited 31 July 2006).
46. 'ID card database 'not for sale'', 26 June 2005 (http://news.bbc.co.uk/1/hi/uk_politics/4624735.stm, 31 July 2006).
47. KST 25764, 018, KST59219.
48. 'Hackers Clone E-Passports', 3 August 2006 (http://www.wired.com/news/technology/0,71521-0.html?tw=wn_technology_security_4, visited 31 August 2006).
49. http://www.rfid-paspoort.nl (visited 6 September 2006).
50. http://forum.scholieren.com/showthread.php?s=da6ff22eaf2e0c6986400111eb6e20eb&threadid=1461229 (visited 6 September 2006).
51. http://www.kraak-forum.nl/viewtopic.php?t=3127&sid=903b5e8c41f7e1dd7b3f5a6c07f413ef (visited 6 September 2006).
52. 'Lachen mag best, geen gekke bekken', AD, 2 september 2006 (http://www.ad.nl/binnenland/article593393.ece, visited 6 September 2006).
53. 'Babymondje moet dicht op pasfoto', AD, 2 September 2006 (http://www.ad.nl/binnenland/article593394.ece, visited 6 September 2006).
54. 'Scans nieuw paspoort mislukken', AD, 1 September 2006 (http://www.ad.nl/binnenland/article589867.ece, visited 6 September 2006).
55. 'Chaos pas is compleet', AD, 1 September 2006 (http://www.ad.nl/binnenland/article589933.ece, visited 6 September 2006).
56. 'RFID-paspoort laat bom afgaan' (http://tweakers.net/nieuws/43817/, visited 6 September 2006).
57. 'Most member states miss deadline for new e-Passports', 31 August 2006 (http://euobserver.com/?aid=22304, visited 7 September 2006).
58. http://retecool.com/forum/threads.php?id=17273_0_19_0_C (visited 6 September 2006).
59. 'Nieuwe paspoort maakt de wereld niet veiliger', 25 August 2006 (http://www.parool.nl/nieuws/2006/AUG/25/bin1.html, visited 31 August 2006)
60. http://indymedia.nl/nl/2006/08/38054.shtml (visited 7 September 2006).

Case #29: AMC hospital

Case ID	# 29, level 1
Title	AMC
Researcher	Christian van 't Hof and Jesica Cornelissen
Timing	2006
Geography	Amsterdam, the Netherlands
Environment	hospital
Technology	Passive RFID tags, PDAs
Maturity	pilot
Function	Matching patients to bloodbags
Owner	AMC
Maintainer	AMC
Users	patients
Other actors	Docters and nurces
Case story	This is a trial with three RFID applications: tracking medical personnel, patients and objects (bloodbags, instruments). When a patient arrives at the hospital he or she receives an RFID bracelet. This bracelet makes it possible for hospital staff to identify the patient and to access medical records quickly and apply treatment with more accuracy. Also, blood bags are tagged by the hospital. All patient records and blood supply information are held on a secured database, which can be accessed by medical personnel through a PDA. Medical records are constantly updated, based on the reading of the PDA's.
ID issue	Besides matching and error prevention of blood transfusion materials, individuals working in the operation rooms (OR) are identified and localised, as well as OR-materials.
Sources	1. 'Zorgsector start proef met RFID.' (http://www.rfidnederland.nl/Default2.aspx?tabid=264, visited 13 september 2006) 2. Garfinkel, S. & Rosenberg, B. (ed.) (2006) RFID: Applications, Security and Privacy. Addison-Wesley.

Case # 35: Selexyz Scheltema SmartStore

Case ID	# 35 , level 2
Title	Selexyz Scheltema SmartStore
Researcher	Jessica
Timing	April 2006 - present
Geography	The Netherlands (Almere)
Setting	Shopping
Environment	Bookstore (warehouse-to-consumer supply chain)
Technology	Rafsec 'Shortdipole2' UHF passive RFID tags by UPM Ralflatac, readers by CaptureTech and software applications by Progress. This provides a total back-office system called Atlas. The software system consists of Progress OpenEdge platform, Apama Event Stream Processing, Sonic Enterprise Service Bus), Progress EasyAsk [1, 12, 16].
Maturity	Operational
Function	Tracking and Tracing of products
Owner	Selexyz Bookstore (formerly Boekhandels Groep Nederland (BGN))
Maintainer	Progress Software Corporation
Users	Suppliers, customers and clerks of the bookstore
Other actors	- UPM Raflatac > supplier of tags [6] - Progress Software Corporation > design of software [7] - CaptureTech > supplier of readers [8] - 3Com > wireless components [9] - Centraal Boekhuis > supplier of books [10]
Case story	The system was introduced to reduce costs in labour, to improve stock control, to make the supply chain more transparent, to increase purchases and to enrich customer experience. Item-level tagging does not only serve the store in streamlining the supply chain and inventory management, it also serves the customers through specially designed information kiosks in providing information on the whereabouts of a book and in offering the possibility to place orders [1, 3]. Selexyz is planning to introduce RFID in a second store in The Netherlands later in 2006 and in the future even in more of its 42 stores in the country [2, 5, 13, 15]. Approximately 38,000 items are tagged. In their leaflet, the store claims that only product-information is stored on the chip. [3, 14, 17] An employee places an unopened box with RFID tagged books into an RFID 'tunnel', which is equipped with a reader. This checks the tags against an electronic record of an advanced shipping notice forwarded earlier over the Internet by Centraal Boekhuis. If there is a discrepancy, the system automatically sends an alert to rectify the order. Checked-in books are placed on store shelves and other displays, with their exact location scanned by employees with handheld RFID scanners. This gives clerks and customers an instant look at a book's exact location as well as its availability. Besides this, the RFID technology enables the store to check inventory more often [4, 11, 12]. The company made several measures as to prevent negative developments. The ICT manager of the store said this was done intentionally; 'in this stage we restrict ourselves to product-information solely, because of possible privacy issues.' They proclaim not to link purchase information with specific customer information and when a book is bought, the chip is deactivated by store personnel. [16, 18]. In an interview with the ICT manager it became clear that the RFID environment is still under construction. There are plans to extend some applications further in the near future, mainly that of security and stock replenishment. It appears that these plans will have no consequences on privacy. Mr. Vink also mentioned to be considering the development of other applications in the

	long run, like narrow-casting and other Customer Relationship Management schemes. This should bring sales up by enhancing cross-selling and up-selling [18]. Mr. Vink says the store did not receive any complaints on the introduction of RFID from their clientele. With regard to the store personnel he says they are 'passively sceptical' and it seems as though operational issues are the basis for this [18]. When the store opened its doors in the beginning of 2006, a member of the BGN management board envisioned a more extensive interpretation of the technology, compared to the current situation. He mentioned the possibility to link the tags to screens in the shop to display information or advertisements. Naturally, it is not prohibited to use smart marketing techniques in your own store, but this method seems to be somewhat more invasive, with screens lighting up when a client picks a certain book from a shelf. Currently, the store has no such displays and, relying on their precautious strategy, they will not come in the near-future. In fact, the customer hardly notices the tags and only the leaflet on the RFID tags and the 'beep' after paying for an item reminds of their presence [3, 16, 17].
ID issue	Item-level tagging is quite well accepted for distribution and logistics application. However, the use of it in stores brings about controversy over privacy. In order to avoid negative sentiment, it is important to be very clear on the nature of data on the chips and the purposes of the system.
Sources	1. 'Progress Software pioneers retail automation with first item-level RFID and SOA deployment'. 19 April 2006 (http://www.computerworld.com.au/index.php/id;1836075961, visited 1 August 2006) 2. Malykhina, E., 'BGN is one of the first merchants to tag individual books, in a new line of stores branded "Selexyz." ' In: InformationWeek, 19 June 2006. (http://www.informationweek.com/story/showArticle.jhtml?articleID=189401951, visited 26 June 2006) 3. 'Besteld boek in Almere belt zelf met klant'. 26 April 2006 (http://www.volkskrant.nl/economie/article294564.ece/Besteld_boek_in_Almere_belt_zelf_met_klant, visited 20 June 2006) 4. Demery, P., 'With RFID tags on each book, Netherlands` BDG chain gives new meaning to speed-reading'. (http://www.internetretailer.com/internet/marketing-conference/74189-rfid-smartstore.html, visited 1 August 2006) 5. Peteghem, L. van, 'Boekhandel Almere koploper met RFID'. In: Automatisering Gids, nr. 27, 2006 6. http://www.rafsec.com/homeb.html, visited 30 August 2006 7. http://www.progress.com (visited 1 August 2006) 8. http://www.capturetech.nl/ (visited 1 August 2006) 9. http://www.3com.com (visited 1 August 2006) 10. http://www5.cbonline.nl/vni/html/ (visited 1 August 2006) 11. Vink, J. and Smit, M., 'Een RFID chip op elk product in een boekenwinkel'. 24 May 2006. Rotterdam, Emerce (http://www2.emerce.nl/downloads/selexyz.pdf, visited 1 August 2006) 12. 'First RFID Item-Level Tagged Store Opens'. 26 April 2006 (http://www.rfidupdate.com/articles/index.php?id=1103, visited 1 August 2006) 13. 'Uitgebreide rfid-proef in Almeerse boekhandel succesvol' (http://tweakers.net/nieuws/42763/Uitgebreide-rfid-proef-in-Almeerse-boekshop-succesvol.html, visited 19 July 2006) 14. 'Slimme boekwinkel draait op RFID'. In: Automatisering Gids, no. 17, 27 April 2006 15. Songini, M. L., 'Dutch bookseller creates item-level RFID system'. In: Computerworld, 8 May 2006 16. Personal observations in Selexyz Scheltema Bookstore on 29 august 2006 17. 'Nieuw. In onze winkel heeft elk boek zijn eigen chip.' (leaflet provided in the Selexyz Scheltema bookstore) 18. Interview with Mr. Jan Vink, ICT manager of BGN, on 13 september 2006

Case #36: KidSpotter Child tracking application

Case ID	36 , level 3
Title	KidSpotter Child tracking application
Researcher	Jessica Cornelissen
Timing	Launched on 27th March 2004 in Legoland Billund, Denmark
Geography	Denmark
Environment	Leisure
Technology	The Child tracking application involves four elements, which combines technologies from Theme Park Intelligence KidSpotter [13] and Aeroscout [14]: - T2 tags incorporated in a wristband or a badge clip. The technology combines active RFID detection with a Wireless LAN environment. The tags make it possible to locate any asset normally not Wi-Fi enabled and is 802.11b compatible. The tag has a battery life of 3 years and weighs 35 grams. - location receivers are placed throughout the park; roughly 40 to 50 location receivers are to be installed throughout an 150.000 square meters park. These remotely configurable receivers are housed in rugged NEMA-rated weatherproof enclosures. They can be connected to the park's network by fiberoptic cable links and wireless bridges. - location server software, installed on a server with Intel Xeon processors. The core software, written in C#, manages the collection and processing of location data. - mobile communication platform handles the communication between the KidSpotter applications, the location server and the SMS gateway that sends up-to-date location information to visitors' mobile phones. [13, 2, 16, 18]
Costs	The rental fee is €3 per day; (in comparison: the entrance fee is mid-€20s) Installation of a location receiver costs $3,000 to $4,000 each. The tags cost appr. $85 each and the park is starting with 500 of them [15]
Maturity	Fully implemented
Function	1. A tracking and alerting system for parents 2. An information system for park management (real-time location service)
Owner	Legoland Billund
Maintainer	Legoland Billund
Users	Visitors of the theme-park
Other actors	
Case story	The system was developed to address the need of the amusement industry to have insight in visitor movements. But it also addresses another problem; the (temporary) loss of about 1600 children annually, that is 0,1% of their visitors. On entering the park the parents can choose to make use of the system by paying a rental fee for the tag. They then register the tag by associating their mobile phone number to the tag-ID and they receive a (gridded) map of the area. If the parents lose sight of their child, they can send an SMS message to the Kidspotter system. They will receive a return message stating the name of the park area and the map coordinate of their child's position in the park with an accuracy of 3 meters. When leaving the park the tag is deactivated so it can be re-used. All data is stored in an open format to enable extensive data analysis of visitor behaviour and the park's most popular routes. Because of this format, it is possible to run both standard tests and specific tests designed by the park management. The system is tested by Legoland Billund in 2004. The British branch in Windsor might be installing the system too, according to Ben Egan, Windsor spokesman [19].
ID issue	Obtaining information about movement of visitors in the park by coupling it to a popular service (without them knowing it?).

Sources	13.	http://www.kidspotter.com (visited 26 June 2006)
	14.	http://www.aeroscout.com (visited 26 June 2006)
	15.	Collins, J., 'One of Europe's largest amusement parks deploys a Wi-Fi-based RFID system that helps parents retrieve children who have wandered off.' In: RFID Journal, 28 April 2004.
	16.	'Child Tracking Application at LEGOLAND: customer case study.' AeroScout
	17.	'Legoland volgt kinderen met RFID-armband' In: Automatisering Gids Webeditie, 25 June 2004.
	18.	'AeroScout Visibility System Overview: data sheet.' AeroScout
	19.	Nash, E., 'Legoland builds safety system for kids: Windsor theme park could follow the lead of its Danish counterpart.' (http://www.iwr.co.uk/computing/news/2070665/legoland-builds-safety-system-kids, visited 26 June 2006)

Case #56: OV-chip Kaart

Case ID	56, level 3
Title	OV-chip Kaart
Researcher	Christian van 't Hof/ Sil Wijma
Timing	2005-2007
Geography	The Netherlands
Environment	Public Transport
Technology	ID card with passive tag, rewriteable Readers installed at the entrance and exit of the different means of public transport. Central database controls payments and profiles travellers. East West builds and maintains the system [22, 34].
Costs	Starting costs: according to one source more than one billion euro [8]. The total costs are probably around 1,5 billion euro [33]. The government only pays a small part of this: the pilots were supposed to cost €7,8 and the total implementation €90 million [23]. Later more money was needed up to a total of €129 million [38].
Maturity	Different pilots. A pilot runs in the city of Rotterdam, while the card will be implemented in the whole Dutch public transport system in 2007.
Function	Payments
Owner	Trans Link Systems (TLS), a consortium of the five larges public transport companies in the Netherlands, representing 80% of the Dutch market.
Maintainer	East West
Users	Dutch users of the public transport, trains, busses, subway, etc.
Other actors	- Different organisations: CBP (College Bescherming Persoonsgegevens), Landelijk Overleg Consumentenbelangen Openbaar Vervoer (Locov), Landelijke Campagneteam invoering OV-chipkaart (Lcov), EastWest - Different consumer organisations: Consumentenbond, Rover, Bits of Freedom - Different public transport operators: NS (Dutch Railways), TLS, GVB, RET, Connexxion, HTM, Mobis
Case story	The OV-chip card is a RFID card system for all forms of public transportation in the Netherlands; bus, tram, metro, train and ferries. The Netherlands is the first country to introduce such a nationwide public transport system for access and payment. The system is based on the Octopus system of the city of Hong Kong, where the system works quite well. The London Oyster card is another example that is very similar. The introduction of the OV-chip card will be done per region because research showed that an immediate nationwide introduction was not possible [21]. Before the nationwide introduction of the OV-chip card different pilots are held [30, 52]. The first pilot was on a ferry service and started on 13th December 2004 [21]. Another important pilot is running since 2005 in Rotterdam with 30.000 test travellers. The pilots were meant to see if a nationwide introduction of the OV-chip card is possible [21]. The tests showed that there are different issues to be solved before a nationwide introduction is possible. Many technical difficulties occurred, urging the pilot into overruns and countering efficiency claims [27, 28, 29, 31]. But the minister still decided to continue the introduction of the OV-chip card [38, 51]. Therefore a second round of pilots was started to develop more experience and simplify the nationwide introduction [21]. In the summer of 2006 the Amsterdam metro system started a pilot by giving 30.000 travellers an OV-chip card. Different members of parliament emphasize the need of a good information campaign to inform the public about the OV-card [25]. Because of the problems encountered in the pilots the introduction of the nationwide system is postponed with one year and should be in use before the 1st of January 2009 [38]. Privacy An important issue in the introduction of the OV-chip card is privacy. In February 2006 the CPB (the Dutch council on privacy matters) warned the NS (Dutch Railways) and other public transport corporations that the storage and use of travel information is not always legitimate [5]. The CBP states that the aggregation of data has to be limited to the necessary data. But public transport organizations want to collect as much data as possible for direct marketing and to get detailed insight in the use of the public transport [4, 5]. According

	to the CBP commercial purposes alone are no reason to store and use data. The question hereby is whether travellers have a fair opt in or opt out choice. According to the WBP users explicitly have to agree with the collection and storage of travelling data [4]. But it looks like travellers don't always have a clear choice. In case of the discount card of the NS for example the users agree with the collection of data when they first use the card. Consumer organizations say that this is the wrong way round; the standard should be that travellers don't give permission unless they actively say TLS can use their data. The CBP also warned against personal cards that are (temporarily) cheaper than anonymous cards [41]. And finally there are questions concerning the storage term of the gathered data. The companies have to respect the law on the protection of personal data (Wet Bescherming Persoonsgegevens, WBP). But the NS and TLS say they interpret this law differently than the CBP does and still say they can store and use the data. The minister of transport still hopes to solve the issue [39, 40, 50]. Costs Another problem occurs with the different possibilities of the OV-chip card. This card can be loaded with a certain product (like a train ticket), which is called 'specifying beforehand'. Another option is to check in with the card at the entrance and checking out at the exit, known as 'specifying while travelling'. Consumer organizations find it unacceptable that 'specifying while travelling' is going to be more expensive than 'specifying beforehand' namely 10 to more than 100 percent [13]. Then most travellers will specify their journey beforehand thus limiting the advantages of the OV-chip card. According to calculations the costs of travelling in rush hours will rise with 10% while travelling outside these hours will cost 20% less [12]. Consumer organizations protest against this because most travellers have no choice but to travel during rush hours [14]. Apart from travelling costs there are also costs to obtain a chip card. Some members of parliament and different consumer organizations like Rover find the price of the card (€7,50) too high [17, 20, 25, 26]. This resulted in a temporarily lowering to €3,75 [38]. But according to the consumer organizations a temporarily low price is insufficient [17]. Members of the parliament also warned that the travelling costs should not rise with the introduction of the OV-chip card, the minister agrees [28]. Another issue is that TLS profits from the interest from the balance on the cards, this could be used to lower the price [36]. Consumer organizations further want to use more possibilities of the OV-chip card to maximize its utility and acceptance of the travellers (lockers, station stores, parking, train taxi) [13]. But for now it is unclear what the possibilities are. The website of the OV-chip card even states that mobile phones and other RFID-cards can cause malfunctioning of card readers [9]. Although there have been a great number of pilots worldwide on the use of RFID systems the use in practice is first to been seen. An evaluation showed that 75% of the travellers that use the OV-chip card say the system works sufficient, 25% thinks there are to many problems with malfunctioning of the system, limited use and costs that are expected to rise [18]. In June 2006 the parliament and consumer organizations still have worries about the privacy and the costs of the system and costs of travelling but eventually lets the minister continue the project [38, 40]. Reactions on the internet show that people are not convinced about the use of the OV-chip card system. Test travellers say travelling is more expensive with this card and the entrance to the public transport is slower [53]. Other test travellers in Rotterdam praise the system because it is easy to use because you just have to wave your card before a reader [54]. So the test travellers have different opinions about the use of the OV-chip card. But many are scared by the idea that more and more information about their person and whereabouts are registered [54]. Some especially criticise the lack of choice; when using the public transport regularly - and therefore use a discount card or a subscription - they cannot travel anonymous [54]. There are also fears of function creep; that the police soon will get access to all travel data and that the storage term will be extended [54]. And others worry about the security of the travel data, especially when this data will be accessible over the internet [54]. Further there are concerns about the use of the data for commercial purposes like advertisements [55]. Because of these worries people already search for ways to undermine the system; for example by exchanging OV-cards [54]. Other contributors on the internet fantasize about hacking the chip [55]. Another reaction came from a person who is afraid that the use of the OV-chip card for small payments in cinema's, parking lots, etc. (like the system in Hong Kong) combined with an automated reload function of the card balance will cause users to run into debts [55]. And finally there are people worried that the OV-card system is to complex for a large group of people, especially elderly [56]. Personal experiences of our researchers [57]

	In order to get an OV-chipkaart ourselves we needed to fill in an application form requesting many personal details: name, address, bank account, signature and a copy of our passport. This is quite surprising, as the card is a debit system and not a credit system. Money can be put on the card through machines placed at the stations and we did not see why identification was necessary. According to Translink Systems anonymous card should also be available in time, these were not offered yet. Another OV-chipkaart was sent automatically to us by the Dutch Railways, replacing a discount card we already possessed and for which we already provided personal data. The accompanying letter proclaimed we were now "prepared for a new way of travelling". It also stated that, once we waved our card the first time at the reader, this act would be interpreted as an opt in for the user agreement. For details on this agreement we were referred to a website. Although this action can be interpreted as service in order to make the transition more smooth, it is a subtle way to get a personalised card more accepted than the anonymous card. On the subway, the OV-Chipkaart worked quite well. When holding our card near the Translink sign, the reader bleeped, displayed the current value of the card, stated we had checked in and wished us a pleasant journey. We did however not have to use the card to open the gates. These were left open for people still using the paper-based tickets. On the buses however many problems occurred. Sometimes we could not check in. The readers just gave a mysterious code: 707. Most of the bus drivers could not handle the malfunction, made some jokes about them and offered us a free ride. On other occasions, the readers did not sufficiently check us out, resulting in a payment for as far the bus would go. One of our researchers made 40 trips and accounted more than of the transactions failed. A bus driver, helping her out on many of these events, called her one night at home to inquire if everything was sorted out with the card. This account demonstrates the link between the card and the personal information in the database has not been sufficiently secured yet. Finally, at one occasion we were checked for fare dodging by a controller with a hand held reader. We then found out the data on the card also contain our date of birth – yet another bit of identity being managed by the maintainer without our consent.
ID issue	The OV-chip card is used both for payment and profiling traveller's behaviour. Users have two choices in managing their identity: being profiled while travelling with an personal card or anonymous travelling with an anonymous card and fewer possibilities. The case revolves around the question whether travellers have a fair and clear opt in or opt out choice.
Sources	01. "NS schendt privacy" In: Volkskrant. 20 February 2006. 02. 'CBP legt OV-chipkaart aan banden'. In: Bits of Freedom nieuwsbrief, Nr. 4.5, 6 March 2006 (http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_5.html , visited 29 June 2006). 03. 'Pechtold ziet geen problemen met RFID'. In: Automatiseringgids, 11 May 2006 04. CBP 'Visie CBP chipkaart', 16 November 2005 (http://www.cbpweb.nl/downloads_overig/z2004-0850_ov_chipkrt_visie_CBP.pdf?refer=true&theme=purple, visited 20 June 2006). 05. CBP 'brief over chipkaart' (http://www.cbpweb.nl/downloads_uit/z2004-0850.pdf?refer=true&theme=purple, visited 20 June 2006). 06. 'Waarom vertrouwen jullie de klant niet?'. In: Volkskrant, 20 February 2006 (http://www.volkskrant.nl/binnenland/article224714.ece/Waarom_vertrouwen_jullie_de_klant_niet , visited 20 June 2006). 07. Ejure.nl, 'Commentaar eJure op de OV chipkaart' (http://www.ejure.nl/mode=display/downloads/dossier_id=49/id=371/Commentaar_eJure_op_de_OV_chipkaart.pdf, visited 26 June 2006). 08. 'OV-chipkaart ook in Amsterdam te gebruiken', 31 July 2006 (http://www.clubmetro.nl/index.php?actie=nieuws&c=2&id=61561, visited 2 August 2006). 09. http://www.ov-chipkaart.nl (visited 22 June 2006). 10. http://www.verkeerenwaterstaat.nl/Images/G0-besluit%20OV-Chipkaart_tcm195-160470.pdf?dossierURI=tcm:195-15678-4 (visited 26 June 2006). 11. 'Ook tram-, bus- en metrovervoer wil gegevens opslaan'. In: Telegraaf, 21 February 2006 (http://www.telegraaf.nl/binnenland/33944341/Ook_tram___bus__en_metrovervoer_wil_gegevens_opslaan.html (visited 26 June 2006). 12. 'Spitsreiziger 10 procent duurder uit'. In: De Volkskrant, 11 April 2006 (http://www.volkskrant.nl/binnenland/article278824.ece/Spitsreiziger_10%C2%A0procent_duurder_uit , visited 11 July 2006). 13. LOCOV (2005) Advies kaartproposities OV-chipkaart, 26 April 2005, http://www.minvenw.nl/cend/overlegorganen/locov/uitgebrachte_adviezen/2005/Index33.aspx#0 (visited 23 June 2006). 14. 'OV-chipkaart mag vervoer niet duurder maken', 12 April 2006 (http://www.consumentenbond.nl/nieuws/nieuws/Archief/2006/4093170?ticket=nietlid, visited 11 July

2006).
15. 'Consumentenorganisaties willen uitstel besluit OV-chipkaart', 11 May 2006 (http://www.consumentenbond.nl/nieuws/nieuws/Archief/2006/4339524?ticket=nietlid visited, 11 July 2006).
16. 'Doorgaan met OV-Chipkaart', 28 June 2006 (http://www.rover.nl/nieuws/berichten/berichten.php?id=ber060629, visited 11 July 2006).
17. 'Extra jaar voor invoering OV-chipkaart hard nodig', 13 June 2006 (http://www.rover.nl/nieuws/berichten/berichten.php?id=ber060613, visited 11 July 2006).
18. 'Als de poortjes maar hufterproof zijn'. In: NRC Handelsblad, 30 May 2006 (http://www.nrc.nl/binnenland/article335132.ece, visited 22 June 2006).
19. The chip card for public transport in The Netherlands. 2004, EastWest (http://www.eastwestconsortium.nl/downloads/presentation.pdf , 28 July 2006).
20. Kamerstuk 2003-2004, 23645, nr. 061
21. Kamerstuk 2003-2004, 23645, nr. 074
22. Kamerstuk 2003-2004, 23645, nr. 074, Bijlage 2511
23. Kamerstuk 2004-2005, 23645, nr. 078
24. Kamerstuk 2004-2005, 23645, nr. 078, Bijlage 3135
25. Kamerstuk 2004-2005, 23645, nr. 084
26. Kamerstuk 2004-2005, 23645, nr. 085
27. Kamerstuk 2004-2005, 23645, nr. 088
28. Kamerstuk 2004-2005, 23645, nr. 093
29. Kamerstuk 2004-2005, 23645, nr. 095
30. Kamerstuk 2004-2005, 23645, nr. 101
31. Kamerstuk 2005-2006, 23645, nr. 111
32. Kamerstuk 2005-2006, 23645, nr. 114
33. Kamerstuk 2005-2006, 23645, nr. 119
34. Kamerstuk 2005-2006, 23645, nr. 123
35. Kamerstuk 2005-2006, 23645, nr. 135
36. Kamerstuk 2005-2006, 23645, nr. 136
37. Kamerstuk 2005-2006, 23645, nr. 139
38. Kamerstuk 2005-2006, 23645, nr. 141
39. 'Stand van zaken invoering OV kaart' (http://www.verkeerenwaterstaat.nl/Images/br%2E873%20stand%20van%20zaken%20invoering%20OV-Chipkaart%20-%20%20%20%20www%2Everkeerenwaterstaat%2Enl%20cend%20bsg%20brieven%20data_tcm195-134235.pdf?dossierURI=tcm:195-15678-4, visited 26 June 2006).
40. 'Strippenkaart wordt OV-chipkaart'. In: Trouw, 28 June 2006 (http://www.trouw.nl/laatstenieuws/In_binnenland/article362227.ece/Strippenkaart_wordt_OV-chipkaart?backlink=true (29-06-06).
41. RET verzamelt reizigersinfo met chipkaart'. In: AD, 18 June 2006 (http://www.ad.nl/rotterdam/article413455.ece , 22 June 2006).
42. 'Reactie van CBP op E-jure over OV' (http://www.ejure.nl/downloads/dossier_id=49/id=371/show.html , visited 26 June 2006).
43. 'Axalto selected for world's first national project covering all transport modes', 27 July 2004 (http://www.rfidnews.org/news/2004/07/27/axalto-selected-for-worlds-first-national-project-covering-all-transport-modes/, visited 28 July 2006).
44. 'Nederland open voor OV-chipkaart', 11 november 2003 (http://www.tns-nipo.com/, visited 11 July 2006).
45. KST 23645, 141, bijlage 1
46. KST 23645, 141, Bijlage 2
47. KST 23645, 141, Bijlage 3
48. KST 23645, 141, Bijlage 4
49. KST 23645, 141, Bijlage 5
50. KST 23645, 141, Bijlage 6
51. 'OV-chipkaart van start zonder duidelijkheid over privacy'. In: Bits of Freedom nieuwsbrief, Nr. 4.13, 21 June 2006 (http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_13.html, visited 31 July 2006).
52. http://nl.wikipedia.org/wiki/OV-chipkaart (visited 1 September 2006).
53. http://forum.trosradar.nl/viewtopic.php?t=24738&postdays=0&postorder=asc&start=30&sid=53f4c33df9a33cdf31dcc10abc280711 (visited 8 September 2006).
54. http://tweakers.net/nieuws/43150/Bits-of-Freedom-twijfelt-aan-privacywaarborgen-OV-chipkaart.html

	(visited 8 September 2006). 56. 'Ov-chipkaart vernietigt sociaal kapitaal', 26 June 2006 (http://www.refdag.nl/artikel/1265566/Ov-chipkaart+vernietigt+sociaal+kapitaal.html , visited 8 September 2006) 57. Several site visits by Christian van 't Hof and Chris de Jongh

Case #61: Transport for London (Oyster card)

Case ID	61, level 1
Title	Transport for London (Oyster card)
Researcher	Christian van 't Hof/ Sil Wijma
Timing	2002-2006
Geography	London, UK
Environment	Public transport
Technology	Philips Semiconductors' MIFARE Standard 1 Kbyte ICs in G&D and SchlumbergerSema cards [3]
Maturity	Fully operational
Function	Payment
Owner	Transport for London, TranSys
Maintainer	Who maintains the database and readers?
Users	Who uses the RFID tags to move through the environment
Other actors	TranSys (consortium of Cubic, EDS, Fujitsu and WS Atkins), Transport for London (TfL) and London Underground Limited (LUL)
Case story	The Oyster card is a RFID-card for public transport in London. It can be used on trains, trams, busses, metro and Docklands Light Railway (DLR). A Travelcard or Bus Pass season ticket can be loaded on it, as well as travel value (cash) to pay as you go [1]. Reloading is possible via ticket offices and machines, over the Internet and by telephone [1]. In London there are nearly seven million bus and Underground journeys every day [3]. The Oyster card was introduced in August 2002 for staff [3]. Using a Oyster card to 'pay as you go' is cheaper than buying paper tickets [2]. The 'pay as you go' service was introduced in January 2004 [2]. Over 5 million people use a Oyster card [4]. A refundable deposit of a little over €4,- has to be paid when purchasing a Oyster card (unless at least a monthly ticket is loaded to the card). Without registration the Oyster card is restricted in such a way that only 'pay as you go 'and weekly tickets can be loaded [2]. The 'pay as you go' service is not available on all public transportation in London; now most railroads in London do not use the Oyster system. In 2008 this should be the case. A 'capping' system was introduced on 27 February 2005, which guarantees that an Oyster card user will be charged no more than the cheapest combinations of single tickets, travelcards and/or bus pass that cover all journeys made that day. [2]. Although there have been different plans to use the Oyster card for small payments [6] TfL now says it is to complex to realise this []. Due to a malfunctioning of the system it has been out of use for one morning [7]. Another bug made travelling impossible for some cardholders for some time [2, 8].
ID issue	When purchasing the Oystercard, full personal detailes are required [11] The police in very interested in using the journey data that is stored from travellers who use the Oyster card. The number of request from the police has risen from seven in 2004 to 61 requests made in January 2006 alone [4]. A spokesman of TfL said: "Transport for London complies fully with the Data Protection Act. Information on individual travel is kept for a maximum of eight weeks and is only used for customer service purposes, to check charges for particular journeys or for refund inquiries. "A very few authorised individuals can access this data and there is no bulk disclosure of personal data to third parties for any commercial purposes. There is no bulk disclosure of personal data to any law enforcement agency. If information is disclosed, it is always done so in accordance with the Data Protection Act after a case-by-case evaluation. [4].

	People are using the information that is stored from the journeys made with a Oyster card to track their partners' movements. The data is accessible through machines at stations and via a website whereby only the registration number is required. This source states that this data is kept for ten weeks [9].
Sources	1. http://www.tfl.gov.uk/tfl/fares-tickets/oyster/general.asp (visited 27 July 2006). 2. http://en.wikipedia.org/wiki/Oyster_card (visited 27 July 2006). 3. 'Easing travel in London's congested public transport network' (http://mifare.net/showcases/london.asp, visited 27 July 2006). 4. 'Oyster data use rises in crime clampdown', 13 March 2006 (http://www.guardian.co.uk/uk_news/story/0,,1729999,00.html?gusrc=rss, visited 27 July 2005). 5. 'Transport Secretary and Mayor of London announce new Oyster deal' Press Release, 10 May 2006 (http://www.london.gov.uk/view_press_release.jsp?releaseid=8032, visited 27 July 2006). 6. 'Is this end for notes and coins? Patrick Collinson and Tony Levene on the 'tap and go' card', 15 April 2006 (http://money.guardian.co.uk/consumernews/story/0,,1754069,00.html, visited 27 July 2006). 7. ''£50,000 lost' in Oyster failure' (http://news.bbc.co.uk/1/hi/england/london/4335291.stm, visited 27 July 2006). 8. 'Inquiry into Tube's Oyster card', 23 January 2004 (http://news.bbc.co.uk/1/hi/england/london/3422051.stm, visited 27 July 2006). 9. 'And the next witness is..... an Oystercard', 22 February 2006 (http://london-underground.blogspot.com/2006_02_01_london-underground_archive.html#114059551043902945, visited 31 July 2006). 10. http://www.tfl.gov.uk/tfl/fares-tickets/oyster/general.asp 11. User application form: https://sales.oystercard.com/oyster/lul/basket.do

Case #66: Detention Concept Lelystad

Case ID	# 66, level 2
Title	Detention Concept Lelystad
Researcher	Jessica
Timing	January - December 2006
Geography	The Netherlands, Lelystad
Setting	Work
Environment	Prison
Technology	Active RFID-tag incorporated in non-removable bracelets for prisoners [1] and in key-chains for wards. Two types of location measurements are tested: triangular locating and zone locating. triangular locating is developed in a cooperation of KPN, Geodan, Aeroscout and Tsilink Hardware. The zone locating is developed by Transquest and Wavetrend [17]. DJI controls the following applications and/or data [16, 19]: - Selection of activities that inmates can choose - Linkage of an inmate to his/hers wristband - Giving out information about inmates to thirds parties - Managing inmate dossier (checking out of inmates) - Planning of activities - Software for handheld computers (PDA's) - Login into a personal prisoner information system using the wristband
Maturity	Pilot
Function	- Information on inmate's stay (security and monitoring) - Planning of daily schedule - Keeping record of inmate's credits - Information on personnel [17]
Owner	DJI (Penitentiary Lelystad)
Maintainer	DJI's 'Shared Service Centra' [6, 16]
Users	Wards and prisoners enrolled in the trial
Other actors	- Van de Geijn Partners ketenarchitecten > design of total detention concept [2] - Ministry of Justice [3] - DIGIT Touch Systems > supply of touch screens [4] - Geodan (KPN, Aeroscout, Tsilink Hardware) > software and hardware design [5] - Transquest and Wavetrend > software and hardware design [7, 8] - Supporting parties like the food-supplier
Case story	The pilot runs from January 2006 until December 2006. In the pilot several technologies, including RFID are tested in a real environment. This pilot should lead to future options on integrating technology in prison systems. The concept is developed as part of DJI's policy on new ways of detention where prisoners get more responsibility. Besides, it should also save costs and at the same time bring adequate security and safety for inmates and prison personnel [9, 10, 11]. The prison complex is especially built for this pilot and has six-person cells equipped with the necessary technology. A maximum of 150 prisoners, which should have a (remaining) penalty not exceeding four months, can stay in the complex [12, 13]. The tag in the inmates' bracelet generates a signal every 1.5 seconds, generating information about the identity and the location of the prisoner. The prisoner can use his/her tag to design his/hers individual day programme. This is forwarded to the wards. After approval, the programme is transferred to the system, enabling access to certain areas or services. Adherence to the day programme is monitored and an alarm is activated when a prisoner is not following the programme. Furthermore, the system has a crediting and penalty function. These

	event are stored in a digital dossier, which is accessible in a 'static post' or through mobile PDA's [1, 14]. The wards carry an active RFID tag in a key-chain, which gives the control room real time information about their whereabouts. The key-chain has a 'panic button' in case of emergency. When there is a problem on the floor, the control room has in instant overview of the wards' whereabouts and appropriate orders can be given [12]. In Dutch newspaper the prison is being called 'Big Brother bajes' (bajes is Dutch slang for prison) [15]. A visitor of a discussion board commented on an article about the concept: "I also had a major problem with the fact that failure to pay traffic fines or petty theft could land you in a prison like this. That means I, and many others in the class, could have our right to privacy legally stripped from us in a very dehumanizing way if we lived in the Netherlands. I think this kind of surveillance, for petty crimes, is completely backwards of the Dutch, who are otherwise liberal" [18]. The prison wards did not express concerns nor had questions about the technology at first. After a while however, some issues rose, for instance about what happens if somebody visit the toilets. It seems as though realisation of the possible consequences of the technology grew in time and that examples can help in creating this understanding. In addressing these issues, the concept designer and the prison wards reached an agreement not to use any information that could possibly be collected with the RFID environment. According to the designer, this has never been the intention and the agreement stands to take away or avoid any concerns [19].
ID issue	The use of constant surveillance brings some controversy and 'Big Brother-scenario's' can easily be related to this case. Applying it to punish or reward a person goes even further. However, it remains debatable how much privacy rights imprisoned people (should) have. Besides the prisoners being constantly monitored, also the wards are under permanent watch. This brings about a different employer-employee relationship in which the employees' privacy could be impinged. It could be seen as a trade-off between being monitored and being more secured at work. It appear as though realisation of the possible consequences of the technology came in time. Addressing concerns and allowing for a dialogue between employer and employees can facilitate in the acceptance of a new technology.
Sources	1. http://www.wavetrend.net/content.asp?IDS=126 (visited 25 July 2006) 2. http://www.vdgp.nl (visited 27 June 2006) 3. http://www.minjus.nl/ (visited 26 July 2006) 4. http://www.digit.nl (visited 26 July 2006) 5. http://www.geodan.nl (visited 27 June 2006) 6. http://www.dji.nl (visited 26 July 2006) 7. http://www.transquest.nl (visited 22 August 2006) 8. http://www.wavetrend.net (visited 22 August 2006) 9. 'Een nieuwe manier van strafuitvoering' (http://www.dji.nl/main.asp?pid=251, visited 26 July 2006) 10. Stordiau-van Egmond, A.M.E., 'Uitnodiging perspresentatie detentieconcept Lelystad' http://www.perssupport.anp.nl/Home/Persberichten/Actueel?itemId=74217, visited 26 July 2006) 11. 'Prison of the future: Detention Concept Lelystad' (http://www.geodan.nl/en/markets/public-order-and-safety/detention-concept-lelystad/, visited 25 July 2006) 12. 'Modernste gevangenis van Europa voorzien van nieuwste technologie: DIGIT Touch Systems / Creative Action voorzien modernste gevangenis van Europa in Lelystad van nieuwste technologie' (http://www.perssupport.nl/Home/Persberichten/Actueel?itemId=74659&show=true, visited 26 July 2006) 13. Maurits, R. 'Nederlandse gevangenen bewaakt via RFID-chip: ook uitgebreide multimediavoorzieningen in cellen.' 24 January 2006. (http://www.zdnet.be/news.cfm?id=53006&mxp=109, visited 6 July 2006) 14. 'Gevangen in ketens: modernste gevangenis: opvallend resultaat van gedurfde visie.'

(http://www.vdgp.nl/bbcms/assets/pdf%20bestanden/Gevangen%20in%20ketens.pdf, visited 25 July 2006)
15. ''Big Brother Bajes' nu al omstreden'. In: Algemeen Dagblad, 30 May 2006.
16. Bouwman, R., 'Digitale detentie gooit gevangenis 'open''. In: Livre Magazine, February 2006.
17. Personal communications with a representative of Van de Geijn Ketenpartners, 26 July 2006
18. Comment by 'reginav' on 12 March 2006 (https://secure.lsit.ucsb.edu/phpbb/viewtopic.php?t=297&sid=db0cb28e98afac6130a8f66cbb5b9d9c, visited 31 July 2006)
19. Personal communications with a representative of Van de Geijn Ketenpartners, 1 September 2006 and 4 september 2006

Case #84: SI.PASS

Case ID	84 , level 1
Title	SI.PASS
Researcher	Elisabetta El-Karimy
Timing	2006
Geography	Torino, Italy
Environment	Public transport / traffic
Technology	Developed by Norwegian company Q-Free on behalf of the Italian transport operator SITAF, the SI-PASS is a two-piece tag consisting of an on-board unit, called a Transponder Mobipass, and a Smart Card. SI-PASS integrates two payment systems using ASK's TanGO-based CT4002 contactless smart cards and active RFID tags for long-range payments. [6] The Smart Card itself is a readable card consisting of a microchip with a double interface (contact and contactless) that uses tag and beacon technology. Operated by microwave dedicated short-range communications (DSCR) at 5.8GHz, the system is compatible with European standards. Operation of SI-PASS is based on two very simple mechanisms. When the card is used with the Transponder it allows motorway barriers to be opened from a distance without the need to stop at motorway tolls. On its own, the card can be read by a scanner, enabling the user to automatically pay for public city transport (buses, trams and underground) in addition to a large number of car parks. For the Turin Winter Olympics, the card was also used to pay for ski-passes and has the capacity to gain access to other events. [7]
Costs	Customers pay 100-170€ plus 20€ deposit for Transponder
Maturity	Just implemented
Function	Access / payment
Owner	SITAF
Maintainer	SITAF
Users	Visitors to Winter Olympic Games and users of Frejus highway tunnel and the A32 highway
Other actors	ASK, Gruppo Torinese Trasporti (GTT), Societa Italiana Traforo Autostrade del Frejus (SITAF), Centro Ricerche Fiat (CRF, Q-Free ASA (Norwegian company for electronic toll collection systems), city car parks and public transport (Trenitalia and 27 private operators), Torino Turismo (musea, concerts, car- and bike rental, etc.)
ID issue	"This new system will not only help us to combat fraud but also enable us to collect data so that we can offer customized fares and value added services to travelers, says Mr. Aliverti, Sales Director, GTT."[1]. “The Smart Card is very much like the Oyster card that is already employed across London. The difference here is that it can automatically debit users as they travel around a city. Unlike the Congestion charging zone in London, users will not have to make individual payments for each journey they make and can use the card across a number of mobility services.” [7] It is not clear what information will be collected besides data on the movement of vehicles. “We are one of the first companies in the world to offer contactless smart cards for both toll payment and public transport, says Mr. Ugo Jalasse, director, SITAF. The versatility of ASK’s TanGO platform allows us to combine GTT transport services with our own, making public transport at this year’s Winter Olympic Games a smooth and uncomplicated experience.” [1] GTT manages the public transport networks in Torino and its suburbs. Whilst season ticket-holders tend to use new GTT dual interface card, there are 4 different contactless paper tickets (C.ticket®) to meet the needs of other users: a pass for school children, a multimodal pass, a pass for tourists and tickets to museums and galleries. [1] According to the GTT-site the tickets are equipped with magnetic bands [2]. The usefulness of such combination card for payment of toll and public transport beyond the Olympics is not addressed. When purchasing the Torino Card, the customer consents to the processing of personal data: “Personal

	data is collected solely for employment related purposes or for use in connection with other such matters. Personal data shall be disclosed or made accessible to third parties exclusively for the aforementioned purposes. TURISMO TORINO hereby guarantees that anyone may request access to their personal data at any moment in order to up-date, change or supplement such data, and may oppose such data being used for the purposes given above."[8] It is not clear what 'employment related purposes' implies. This disclaimer does not prevent the data of the Torino Card to being passed on to SI-PASS systems. No privacy information is provided on the SI-PASS website. For future use, the possibility has been considered to employ SI-PASS to effect toll payments with the help of satellite technology, such as is already in use for heavy goods in Germany (TOLL COLLECT). The telematic platform has been devised to expand the functionality of the system, in particular to give out information on traffic flow and to integrate with working systems on road security (such as INFONEBBIA). [10] But also other linkages of the SI-PASS transponder with other chipcards can be envisioned, such as could as credit cards and cash cards. [3]
Case story	SI-PASS is a dual interface card for public transport, highway toll payments, car parks, and tickets. It was conceived and introduced in time for the Torino Winter Olympics 2006 to reduce traffic congestion and allow visitors automatic access to Turin and the Olympic events. Presently the SI-PASS system is in use on the A32 Turin-Bardonecchia motorway, the Frejeus tunnel and Turin bypasses, the GTT public city transport services and the GTT park and ride car parks. [7] It will remain as part of the infrastructure of Turin for decades to come. [7] The unified ticketing system provides seamless mobility from SITAF highways toll to city car parks and public transport (Trenitalia and 27 private operators) [1] [3] [6] The system is designed to cut traffic congestion, reduce pollution and allow users automatic access to Turin and the venues for the Winter Olympic' events without the need for manual payment methods. [7] SI-PASS is available in two variations, BronzeA and Bronze B. Bronze A costs 100€ plus 20€ deposit for Trasponder Mobipass and offers: unlimited transit on highway A32 for 5 days; unlimited transit on highway (tangenziale) including the dynamic passage of the Bruere toll station; free parking for 48 hours at GTT parkings Caio Mario e Stura; free public transportation (previous compilation of form needed); free underground; free Olympic shuttles. Bronze B costs 170€ plus 20€ deposit for Transponder Mobipass offering in addition to above mentioned unlimited travel across the Frejus tunnel. [3] Conceived by the Centro Ricerche Fiat (CRF) in collaboration with ANAS, SIPASS is a technological evolution from available systems (such as the Italian TELEPASS or the French T-LIBERTY). [10] The card is a multi-application, multi-modal dual interface card that offers a cluster of services for greater mobility in and around town. SI.PASS is branded with 5 different logos and has already been sent to VIPs and the Olympic family. It will also be available from toll booths and railway stations. With a SI.PASS card, visitors can cruise through automatic tolls on the A32 highway or in the Frejus tunnel and make contactless payments in car parks before boarding on GTT public transport. [1] SI-PASS integrates two payment systems using ASK's TanGO-based CT4002 contactless smart cards and active RFID tags (transponder) for long-range payments. [6] Developed by Norwegian company Q-Free on behalf of the Italian transport operator SITAF, the SI-PASS is a two-piece tag consisting of an on-board unit, called a Transponder Mobipass and a Smart Card. [7] The Transponder Mobipass is a Q-free technology terminal according to European standards allowing dynamic transactions through the use of the Smart Card. Operation of SI-PASS is based on two very simple mechanisms. The transponder needs to be affixed behind the front windshield in the vehicle. When the card is used with the Transponder it allows motorway barriers to be opened from a distance without the need to stop at motorway tolls. The technology allows the establishment of a communication channel and the exchange of information between a moving vehicle and a toll station. [10] The Smart Card itself by ASK is a readable card consisting of a microchip with a double interface (contact and contactless) that uses tag and beacon technology. Operated by microwave dedicated short-range communications (DSCR) at 5.8GHz, the system is compatible with European standards. [7] When inserted in the transponder, it enables the user to pass toll barriers without stopping. On its own, the card can be read by a scanner, enabling the user to automatically pay for public city transport (buses, trams and underground) in addition to a large number of car parks. For the Turin Winter Olympics, the card was also used to pay for ski-passes and has the capacity to gain access to other

	events. ASK cards and tickets are being used by Gruppo Torinese Trasporti (GTT) and Società Italiana Traforo Autostrade del Frejus (SITAF) to drive an innovative ticketing and fare collection system during the 20th Winter Olympic Games. GTT lead the project to provide a pioneering payment system in the Torino region using ASK's TanGO-based CT4002 contactless smart cards and C.ticket® contactless paper tickets. 'The card is compatible with the Calypso system of transport. Adopted by more than 40 cities in various countries, Calypso is a practical standard, safe and in constant development representing the European standard of mobility."[3] [5] Smart cards can be purchased at a number of locations around the city, including the A32 motorway Service Centre at Avigliana, at the Sitaf-Susa information booth, at the A43 motorway toll barrier in Saint Michel de Maurienne, and at the Portanova railway station and Caselle airport outside Turin. [7] The card was available during the 2006 Olympics and Paraolympics, and offered a reduced rate for a combination with the Torino Card (5 € less). [3] [4] [9] The Torino Card, available for periods of 24 or 72 hours or 5 days, allows free access and discount to a number of cultural facilities: (Free travel on all urban and suburban public transport, Free entry in more than 140 museums, exhibitions, monuments, castles, fortresses and Royal Residences in Turin and Piedmont, Free access to the TurismoBus Torino, to the panoramic lift in the Mole Antonelliana,to the Sassi-Superga rack tramway and to the boats on the river Po, Discounts on guided tours, plays, concerts, opera, car and bike rental and much more!) [8] GTT manages the public transport networks in Torino and its suburbs. Whilst season ticket-holders tend to use new GTT dual interface card, there are 4 different contactless paper tickets to meet the needs of other users: a pass for school children, a multimodal pass, a pass for tourists and tickets to museums and galleries. [1] GTT issued five special new tickets on the occasion of the Olympic games, covering the entire area involved in the Games, valid for different services. The tickets are equipped with magnetic band, hologram and bilingual wording, and the graphic design, in line with the new GTT ticketing system in use since the start-up of the new Underground, shows athletes in action in the different Olympic winter sports. [2] SI-PASS is advertised on its own website as an 'efficient instrument, a passe-partout opening doors in all Europe in one movement'. [3] The opening ceremony for the Torino2006 Winter Olympics in February declared a new era for urban traffic schemes with the introduction of the world's first integrated traffic Smart Card system. Oddvar Solemsli, sales and marketing director for Q-Free said: "The Turin project to protect a historic city and to keep traffic moving during the few weeks of the Olympic Games is considered as a flagship model of how an integrated transport model can work. [7] In a world first for contactless technology, ASK delivers a single contactless card for both public transport and highway toll payments. [1] The Olympic traffic challenge serves as a case study for the SIPASS system and, if evaluated successfully, may pave the way for the expansion of the system.
Sources	All visited 14 September 2006 1. ASK.com, producer of card 'Torino 2006 on the Right Track With ASK Contactless Smart Card Technology' http://www.ask.fr/uk/news/news_article.php4?id=3 2. County of Torino where technology was implemented http://www.comune.torino.it/gtt/en/olympicgames/tickets.shtml (visited 05 July 2006). 3. Homepage of SI-PASS device http://www.sipass.it/on-line/Sipass/Home/SIPASS.html 4. On Olympic Games organisation http://www.kataweb.it/spec/articolo_speciale.jsp?ids=1251016&id=1251040 5. On transportation and Olympic Games organisation http://www.radio.rai.it/cciss/view.cfm?Q_EV_ID=162476&Q_TIP_ID=328 6. RFID news Italy homepage http://www.rfidnews.it/news.asp?id=230 7. Q-Free website, Europe's leading supplier of electronic toll collection (ETC) systems http://www.intertraffic.com/marketplace/mypage/pressreleases_detail.asp?mypageid=1102&newsid=581 8. Turismo Torino on Torino Card http://www.turismotorino.org/uploads/4/1925_Torino_Card_2006.pdf 9. http://www.traspi.net/notizia.asp?IDNotizia=7467

	10. Centro Ricerche Fiat http://www.crf.it/C/C7_1.htm

Case #88: Madesjki Smart Stadium

Case ID	# 88, level 3
Title	Smart Stadium Solution at the Madejski Stadium
Researcher	Jessica

Timing	2004
Geography	United Kingdom (Reading)
Setting	Fun
Environment	Stadium

Technology

Smart Stadium Solution developed by Fortress GB [20].

It offers the following modules [46]:

- SmartTicketing
  - Virtual ticket
  - New outlets – scratch card
  - New outlets - kiosks
  - Membership scheme
  - Buy-back scheme
  - Concession upgrades
- SmartAccess
  - Multiple Ticket Types
  - Independent Rule Engine
  - Visual “traffic light” indicators
  - Offline capabilities
  - Dynamic reallocations
  - Evacuation reset
- SmartController
  - Detailed access report
  - Ticket verification
  - Real Time Access reporting
  - White / Watch list
  - Real time card blocking
  - Steward time & attendance
- SmartCRM (Customer Relationship Management)
  - Fan Loyalty scheme
  - Integration with ticketing
- FlowPayments
  - E-Purse
  - Merchandise Kiosks
  - Gift Vouchers

The Madejski stadium uses both plastic RFID cards (member cards and season tickets) and one-off paper tickets (with a bar code or RFID chip). Chips are passive and encrypted. There are RFID readers installed in all the turnstiles [20, 45, 46].

The system software offers the Time Attendance Monitor (TAM) option. TAM gives information on [45]:

- ID-number of the card or ticket
- Name of the carrier
- Time of entrance
- Status of ticket (e.g. access to which game and through which entrance)
- Status of carrier (e.g. blocked card, watch-listed or black-listed person)
- Area and turnstile of entrance

	Some statistical analysis can be done with the TAM, both real-time and afterwards, like [45]: - number of people entering the total stadium - number of entries through each turnstile - division of season passes, member cards and one-time tickets On the ground, there is service personnel equipped with pocket computers (PDA's). These PDA's are linked to the central database through a wireless network, meaning that information is uploaded and downloaded real time. On a PDA, one can access one's card-history by entering the ticket-number. The tickets cannot be read by the PDA using RF [45]. Fortress GB has also developed the so-called Smart Campus Solution and Smart School Solution. These are similar to the Smart Stadium Solution and use the same type of smartcard [20].
Maturity	Implemented
Function	ID / AC / (PA) / IC / IS
Owner	Madejski Stadium
Maintainer	Madejski Stadium, IT department
Users	Supporters, corporate guests and staff of the stadium or clubs playing in the stadium (home clubs of the Madejski Stadium are Reading Football Club and London Irish Rugby Football Club)

Other actors	- Fortress GB's Technology Partners [46]
	
	- Stadiums using the Smart Stadium Solution:
	  - Color Line Stadium in Norway [24]
	  - Headingley Carnegie Stadium in United Kingdom [25]
	  - Åråsen stadion in Norway [26]
	  - Anfield Stadium in United Kingdom [27]
	  - Kiryat Eliezer in Israel [28]
	  - Carrow Road in United Kingdom [29]
	  - Stor Stadium in Norway [30]
	  - JJB Stadium in United Kingdom [31]
	  - Viking Stadium in Norway [32]
	  - Emirates Stadium in United Kingdom [33]
	  - Kristiansand Stadium in Norway [34]
	  - City of Manchester Stadium [35]
	  - Giuseppe Meazza Stadium in Italy [36]
	  - Upton Park (West Ham United FC) [37]
	
	- Venues using the Smart Campus Solution
	  - Bristol City Academy in United Kingdom [38]
	  - University of Hertfordshire in United Kingdom [39]
	  - London South Bank University [40]
	  - Gwernyfed High School in United Kingdom [41]
	  - Little Ilford School in United Kingdom [42]
	  - Thames Valley University in United Kingdom [43]
	
	- Fan clubs [21, 38]

Case story	The Smart Stadium solution consists of a variety of applications operating on one platform. When installing the solution, an owner can choose which application to activate. Other applications can be activated afterwards. Future applications possible with the Smart Stadium solution are: - Mobile ticketing, betting and commerce - NFC-enabled mobile phones for ticketing, access and payment - Offering loyal fans special treatment, based on the profiles held on the membership card - Location based services to monitor location of assets or people in real time [46] The solution was at first introduced at the Madejski stadium for the access and membership applications. Access to the ground is only possible through the RFID operated turnstiles. One person can enter at a time. Personnel working on the ground are equipped with PDA's that give access to the database through a wireless network by entering the ticket number. There are

currently 50,000 member card and season ticket holders. A plastic card costs about 1.20 pounds and a paper ticket is about 0.40 pounds [45, 46].

Currently, the club has embarked on the development of an e-purse system, a loyalty scheme and integration of the RFID environment to other services, like parking or public transport. The e-purse system not only facilitates the transactions executed at the ground, it also gives the stadium management insight in the expenditures of each supporter. This way they can see who are the clubs' 'big-spenders' and link this to their CRM scheme. Finally, it can help to prevent theft by stadium personnel. One of our respondents is quite happy with these developments. He is in favour of extending the RFID environment to the possibility of paying for your drinks and food and paying at the car park [20, 45, 51].

In the stadium there is a Closed-Circuit television (CCTV) environment. Mr. Hanson tells about the possibility of using this to take pictures of supporters or to supervise the ground. Together with the ticketing system, the stadium knows exactly who is sitting at a certain seat. When a supporter is not following the rules or is having a dispute with personnel, the CCTV system can serve as proof and adequate action can be undertaken [45].

The SmartController module makes it possible to observe personnel of the stadium. Also, integration of this module with stewards' payrolls is an opportunity [46, 49]. Though currently not used this way, stewards can get to their workplace without using RFID tokens, Mr. Hanson is being optimistic about the options and is looking into future implementation [45, 47].

The Smart Stadium Solution is used in several other stadiums around Europe. Also, several schools and universities implemented a similar RFID application named the Smart Campus Solution. Because all venues use the same technology, it is possible to integrate them. In Reading for instance, it is possible for students of the Thames Valley University to use their RFID student pass to access the Madejski Stadium [20, 45].

The stadium management obtains data on everyone who visits the venue, which is stored and updated in a supporters' card history. A member cardholder commented on this: "It [retaining and updating the card history, red.] is good so they can see who are the better supporters." Another supporter thinks the level of personal information held at this moment is acceptable, but it should not extent further. His reaction: "I think that games attended and [loyalty] points are a good idea. [..] all the personally information they need is at a correct level but any more will feel a bit like big brother is watching you." [45, 50, 51].

The data in the card history can be informative both in an integrated and in an individual format.Firstly, combining all the data gives insight in statistics. The management can for instance see at what time people tend to enter the stadium and how many regulars and non-regulars visit a match. But it also gives security department insight in the number of people at each stand in case of emergency. Supporters do not seem to mind the fact that this information is generated; all our respondents think it is fine that the stadium collects some information about their supporters, but it should only remain accessible for their football club and not to third parties [45, 50, 51]

Secondly, data in individual card histories can be used for several purposes. For instance to verify claims from supporters. Mr. Hanson gives the example of a supporter re-claiming money for missing part of the game. The card-history can confirm whether this is actually the case. It can also be used in security plans or loyalty schemes. Security department holds and updates watch lists to register unwanted people. When presenting the RFID ticket to the readers in the turnstiles your record is compared to the watch list and access is either granted or denied. Supporters do not seem to mind the use of information for security purposes: "this [link of card history to security department, red.] then helps keep good fans in the club and get rid of troublemakers". Having a loyalty scheme means that the stadium management is actively approaching its visitors; giving them special offers on their birthday, giving them priority on popular matches, asking them why they ended their season ticket or why they did not buy a new away T-shirt this year. This could be experienced as invasive by the targets of these actions. However, when investigating supporters' opinions, this appears not to be the case. A regular of the Madejski said on this "I know they collect my personal information. As long as they use it for football purposes it is fine with me". Another regular commented: "Yes this [link of personal card history to loyalty schemes, red.] is good so you get a benefit for attending

	more matches." A third reply we had on this was: Yes [I agree on the fact that the stadium links personal card history to loyalty schemes, red.] as for each game you attend you get a certain amount of loyalty points given to you and attached to your membership. This then allows you to buy tickets sooner for future matches [20, 45, 47, 50, 51]. Mr. Hanson thinks supporters do have some doubts about using the technology. He thinks it is mainly directed to the technical aspect of the system. He confirms the impression that supporters do not have complaints about the stadium asking for their personal information. According to him, this is probably because (frequent) supporters receive many benefits through the system, not only in terms of convenience but also in terms of commercial benefits. Mr. Hanson thinks, through direct marketing, a supporter not only is being privileged, but also feels privileged. Also one-time visitors experience convenience from giving their personal information as they receive a text-message that states their seat and information on the game [45, 47, 50, 51]. On the use of the information by third parties, our Madejski stadium regulars are less positive. One says not to have any experience with non-football related marketing, but is not certain if this will remain like this: "But they probably also use it [personal information] for marketing purposes. What can you do about it? You can not prove it and you can not change it". Supporters also stated they would want to have a voice in the applications for which personal information or the information gained through the RFID system is used and that he would not want any third party being involved or benefiting from this. Here it must be stated that, according to Mr. Hanson, the information gained in the RFID environment is only used for in-house purposes. The stadium can and will not trade the information to third parties. For one thing, the Data Protection Statement of the register procedure prohibits this and this and other issues about privacy are covered by British Law [45, 47, 50, 51].
ID issue	It seems that the loyalty of the supporter surpasses the will to remain completely anonymous, all for the sake of the game. Supporters are fine with their club using the information and are happy to benefit from it through a loyalty scheme. On the other hand, they do not agree on the use of the system by any third party.
Sources	20. http://www.fortressgb.com (visited 31 July 2006) 21. http://www.backtheboys.com (visited 31 July 2006) 22. 'IBM Case Study: Manchester City Football Club scores a home win with IBM and Software4Sport, part of Computer Software Group.' 18 March 2004 (http://www-306.ibm.com/software/success/cssdb.nsf/CS/DNSD-5X5LK3?OpenDocument&Site=, visited 27 July 2006) 23. Booty, F., 'Reading FC and London Irish Rugby FC keep ahead of the game.' 25 October 2004. (http://www.iseriesnetwork.com/nodeuk/ukarchive/index.cfm?fuseaction=viewarticle&CO_ContentID=19530, visited 27 July 2006) 24. http://www.colorlinestadion.no (visited 23 August 2006) 25. http://www.leedsrugby.com (visited 23 August 2006) 26. http://www.lsk.no (visited 23 August 2006) 27. http://www.newanfield.co.uk (visited 23 August 2006) 28. http://maccabi-haifafc.walla.co.il (visited 23 August 2006) 29. http://www.canaries.premiumtv.co.uk (visited 23 August 2006) 30. http://www.sandefjordfotball.no (visited 23 August 2006) 31. http://www.jjbstadium.co.uk (visited 23 August 2006) 32. http://www.viking-fk.no (visited 23 August 2006) 33. http://www.arsenal.com (visited 23 August 2006) 34. http://www.ikstart.no (visited 23 August 2006) 35. http://www.mcfc.co.uk (visited 23 August 2006) 36. http://www.sansiro.net (visited 23 August 2006) 37. http://www.whufc.com (visited 23 August 2006) 38. http://www.cityacademybristol.co.uk (visited 23 August 2006) 39. http://perseus.herts.ac.uk (visited 23 August 2006) 40. http://www.lsbu.ac.uk (visited 23 August 2006) 41. http://www.gwernyfed-hs.powys.sch.uk/ (visited 23 August 2006) 42. http://www.littleilford.newham.sch.uk (visited 23 August 2006) 43. http://www.tvu.ac.uk (visited 23 August 2006) 44. http://www.lisc.org.uk (visited 23 August 2006) 45. Interview with Mr. G. Hanson, IT manager at the Madejski Stadium, on 2 August 2006

	46. 'Smart Stadium Presentation: brought to you by FortressGB'. Personal communication with Mr. J. Rosenthal, Legal Counsel at FortressGB, on 2 August 2006 47. Interview with a season pass holder and a steward, on 2 August 2006 48. 'Member Card Application' In: Supporters' Guide: premiership 2006/07 49. http://www.stadiacard.com/products/index.php?id=4 (visited 23 August 2006) 50. Interview with a member card holder, on 1 and 11 September 2006 51. Interview with a member card holder, on 9 August and 13 September 2006

Case #91: TopGuard Patrol

Case ID	# 91, level 1
Title	TopGuard Patrol
Researcher	Jessica
Timing	Unknown
Geography	Worldwide
Setting	Work
Environment	Outsourced services (guarding, maintenance, recording service activities, cleaning, attendance [24])
Technology	GCS ProxiPen Data Collection Unit (RFID reader operating at 125 KHz and reading range 3 – 18 mm) GCS TopGuard Patrol reporting software Passive RFID tags on checkpoint and incidents ('Unique' and 'Nova' World Tag) and on personnel (Guard Identification Tag, either a 'ISO Card Unique' magnetic stripe card, 'Tear Shape Unique' key fob or 'Unique' wrist band) by Sokymat [23, 24, 25]
Maturity	Operational
Function	To provide an unfalsifiable record of services which must be performed at predetermined times and places [25].
Owner	Guard Control Systems [25]
Maintainer	Companies executing patrolling services
Users	- Companies and personnel executing patrolling missions - Companies out-sourcing patrolling services
Other actors	- Sokymat, provider of tags [26] - Distributors of the system, worldwide
Case story	The ProxiPen reads RFID proximity tags strategically located around the premises to be toured or fixed to equipment that is due to be inspected. The ProxiPen records the time at which the location was visited and can record simple information related to the location, status or incidents if this is required. The TopGuard Patrol software makes it possible to prepare reports from the downloaded information, including the personnel on the tour, time at which point a control tag was scanned, whether points were missed or duplicated et cetera [23, 25].
ID issue	This application makes it possible for employers to follow employees throughout their shift. This brings has consequences for the relationship between employers and employees.
Sources	23. 'Finally! Proof to back up Service Performance.' (http://www.practicalfm.co.uk/shownews.asp?search_type=id&id=72199, visited 25 August 2006) 24. 'ProxiPen: the New Compact Reader for RFID Tags' (http://iccdata.com/proxipen.htm, visited 25 August 2006) 25. http://www.gcscontrol.com (visited 28 August 2006) 26. http://www.sokymat.com (visited 28 August 2006)

Case #096: NWO Office

Case ID	# 096, level 3
Title	NWO Office
Researcher	Jessica Cornelissen en Christian van 't hof
Timing	2005 - present
Geography	The Netherlands (The Hague)
Setting	Work
Environment	Office building
Technology	Passive, 125 KHz RFID tags (HID ProxKey) and HID MiniProx readers [54]
Maturity	Operational
Function	Access
Owner	Information and system management of the NWO office building
Maintainer	Installerende Partners
Users	Employees at the NWO office building
Other actors	- HID [56] - Installerende Partners [55]
Case story	The system is in use to provide access for people working in both the NWO buildings ('Java' and 'Borneo'). In the building several organisations are resided, occupying different department. Departments have and entrance doors which is equipped with an RFID-lock. The doors to individual offices do not have these locks. To leave the buildings/departments using the tag is not necessary [52]. The data collected using the system is: tag number, name of the bearer, department, time of presenting the tag and door to which the tag is presented. A record of each tag is saved for an unspecified amount of time. According to Mr. Besseling, this is the only information that follows form using the RFID-system and no further analysis is being done [53]. System administrators are responsible for keeping back-ups of the database. This is done weekly by transferring the data to another hard disk. There is no linkage to personnel records or to other sources of information. Formally, only the system administrators are permitted to access the database. However, security levels seem to be fairly low; the data is displayed in a comprehensible manner - time, door, department, name of employee - in the office and the system is not locked by a password. On informing Mr. Besseling about his view on security levels, he says to have no problems with it. In his opinion nobody could have interest in the information that is displayed and moreover, no information is collected that could affect the privacy of the users [53]. Mr. Besseling stresses the fact that the system is only used for access control and not for time registration. He explains that this can not be done, even if he or the institute wanted to, because tailgating is possible and because there is no exit-check. However, he admits that the system can give some insight in the behaviour of the users, especially on the time people start their work. On this, he tells an anecdote about a head of department that wanted to check the starting hours of a certain employee. The employee said to start to work very early every day and, for that reason, could also end the day early. Mr. Besseling said that he did not provide this information when requested, because the system is not meant for this purpose. However, he thinks that if a higher placed person came to him with this question, or if a head of department would persist on receiving the information, he would give it in the end [53]. Mr. Besseling says to have no experience with employees that refuse to use the tags or that have doubts about their privacy. He thinks this is partly due to the fact that most employees traded their old magnetic stripe cards for the new RFID tags. He argues that for the users nothing much has changed and that people see the tags only as a key to open the door to their workplace. Furthermore, employees do not get any information on the tags and the system

	when they collect their tag. According to Mr. Besseling this is not necessary , because 'the tag is only used as an access method and nothing else'. Also, nobody ever asked about the purposes of the system and the information that is collected [53].
ID issue	The system offers several possibilities to track employees more thorough than is being done at this moment. However, management is not using these possibilities. There has been no concern among employees working in the office building. This could be because they are very poorly informed about the system, but another reason could be because the application is accepted as it is right now.
Sources	52. Personal observations 53. Interview with Mr. Cees Besseling, Information and system management, system administrator of the NWO office building, on 18 July 2006. 54. 'Proxkey II' (http://www.hidcorp.com/pdfs/products/proxkey2.pdf, visited 11 september 2006) 55. http://www.ipgroep.nl (visited 11 september 2006) 56. http://www.hidcorp.com (visited 11 september 2006)

Case #108: Liber-T

Case ID	# 108, level 1
Title	Liber-T
Researcher	Jessica
Timing	Unknown
Geography	France
Setting	Car
Environment	Toll roads
Technology	Read/write/re-write tags installed in the vehicle. Reader installed in the entry- or exitgates.
Maturity	Operational
Function	Automatical charging of toll fee.
Owner	The Federation of French motorway and toll facility companies (ASFA) and the French toll-companies (ALIS, AREA, ATMB, Autoroutes Paris-Rhin-Rhone, CCI du Havre, COFIROUTE, ASF / ESCOTA, SANEF, SAPN, SFTRF, SMTPC) [57]
Maintainer	French toll-companies
Users	Subscribers to the Liber-T system (In 2005 there are almost 1,5 million subscribers and there have been 179 transactions per tag per year [58].
Other actors	
Case story	Liber-T is an electronic toll payment system that is implemented on the french tolled motorway (it is also called 'telepeage'). The badge gives drivers the possibility to enter and exit toll-routes through specially designed gates, without stopping and paying with cash or bankcards. The biggest user advantage is shorter queues, this is also the main marketing strategy [57] There is some data on the tag, either fixed or modified. Fixed data is identification of the bearer, the product (subscription type) and the tag. Modified data is observation data on tag status, last entry or exit point and historical data of last 16 entries or exits [62]. On a forum frequently visited by Dutch subscribers to Liber-T, we started a thread on Identity Management in this case. 'MarK' draws a comparison between his bank and his Liber-T subscription. 'They know my address and my bank account (otherwise payment would not be possible). My bank knows this and there are a lot of other people and authorities that know this too.' He also mentions other ways in which personal information can be gathered, like using your creditcard or your cell-phone [63]. This view is shared by other visitors too. ;Mariette 58' thinks it is merely a 'characteristic for this age of time'. This argument appears to make up for the fact that 'they' get to know some things about you [64, 65] 'MarK' closes his response by saying that it actually gives him a feeling of safety in case he got lost on a French highway and adds to this that knowing who you are and where you are going is essential for the company to do its business [63].
ID issue	This system will provide information about the travels a subscriber makes. The information could be used for marketing purposes, though there is no indication that this happens at this moment. It seems that users see the RFID system in perspective to other technologies; there are other ways in which information can be gathered so why cause a commotion over this particular technology? The 'age of time' and 'running the business means knowing things about you' seems to settle doubts.
Sources	57.http://www.autoroutes.fr/asfa/qui.php?lng=2 (visited 7 July 2006) 58.'Key figures 2005: French tolled motorway facilities network.' (http://www.autoroutes.fr/upload/institutionnelle/cles2005-EN.pdf) 59.'Liber-T: the French toll system' (http://www.autoroutes.fr/upload/institutionnelle/telepeagedoc) 60.http://www.sanef.fr/fr/ecommerce/particulier/decouvre.jsp (visited 7 July 2006) 61.French Toll Road Operators (2002) Knowing our costumers

	(http://www.sanef.fr/fr/ecommerce/particulier/decouvre.jsp, visited 14 July 2006). 62.'Liber-T, The French toll system' (http://www.autoroutes.fr/upload/institutionnelle/telepeagedoc.pdf, visited 7 July 2006) 63.Comment by 'MarK' on 4 September 2006 (http://www.frankrijkforum.nl/index.php?link=home/lees.php&id=84195&reactieid=8430 0, visited 5 September 2006) 64.Comment by 'Mariette 58' on 4 September 2006 (http://www.frankrijkforum.nl/index.php?link=home/lees.php&id=84195&reactieid=8430 0, visited 5 September 2006) 65.Comment by 'pwi' on 4 September 2006 (http://www.frankrijkforum.nl/index.php?link=home/lees.php&id=84195&reactieid=8430 0, visited 5 September 2006)

Case #123: VRR/VRS

Case ID	#123, Level 1
Title	VRR/VRS
Researcher	Christian van 't Hof/ Sil Wijma/Eefje Vromans
Timing	2003
Geography	Germany, region of North-Rhine-Westphalia
Environment	public transport
Technology	ASK MV5100 dual-interface contactless smartcards Contactless mode for transit applications (RFID), contacted mode for e-purse application (chip)
Costs	RFID Implementation costs: € 33million [6]
Maturity	Fully operational
Function	Payment
Owner	Verkehrsverbund Rhein-Ruhr (VRR) and Verkehrsverbund Rhein-Sieg (VRS)
Maintainer	Card.etc AG (general contractor) and KompetenzCenter EFM (Automatic fare collection) [?]
Users	Travellers
Other actors	• Transport operators: VRR and VRS represent 54 different transport operators • Card supplier: ASK S.A. • VDV (the association of public transport in Germany) [1] • Foebud e.V. (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V)
Case story	The VRR and VRS are using RFID in trains and busses in the region of North-Rhine-Westphalia in Germany. VRR and VRS, representing 54 different transport operators, cover an area with a total population of 10.6 million inhabitants. VRR, with an extensive bus and rail network, handles 1.1 billion passengers per year. The main cities are Bochum, Dortmund, Dusseldorf, Duisburg, Essen, Oberhausen and Mulheim. VRS handles over half a billion passengers per year. The major cities are Bergisch, Gladbach, Bonn, Cologne (Koln) and Euskirchen. This is Germany's first and Europe's largest rollout of smart cards in public transport [1]. In January 2003 the first RFID cards have been sent to yearly and monthly ticket holders. Eventually the VRR/VRS want to use different kind of tickets: the e-Ticket, e-Purse and e-Market [1]. The main advantage of the e-Tickets is that travellers don't have to buy a ticket anymore. A card reader which is placed in the bus or train registers where the cardholder gets on and off. At the end of the month the costumer gets the bill [4]. By using RFID in public transport it becomes possible to track person's movements [2]. But according to VRS only the relevant data necessary for the validity of the card are stored on the chip: name, validity-date and "zone-validity". No travel details or more personal data are stored [3]. Customers can even choose if they want to pay with a personalised credit card or an anonymous debit card [4]. The card has a Paycard-symbol which guarantees that fraud and misuse of data is minimized [3]. Though, on the internet people discuss how to abuse the tickets [2]. Another source states that in a clothes store in Neuss the data of school kids carrying a 'schoko-ticket' were accidently read out in clear text [5]
ID issue	By using RFID in public transport it becomes possible to track person's movements [2].
Sources	[1] . RFIDnews.org (2003) 'ASK Delivers 1.7 Million Contactless Cards for Largest Transit Smart Card Project in Europe', 21 May 2003 (http://www.rfidnews.org/news/2003/05/21/ask-delivers-17-million-contactless-cards-for-largest-transit-smart-card-project-in-europe/, visited 25 July 2006). [2] http://www.foebud.org/rfid/en/where-find#fahrkarten (visited 06 September 2006) [3] http://www.vrsinfo.de/25598.php (visited 10 September 2006) [4] http://www.breitband-nrw.de/download/050407/20050407-Megger.pdf (visited 10 September 2006) [5] http://www.foebud.org/rfid/en/faq-english [6]http://www.brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_63/PDF/RFID261005.pdf

	(visited 10 September 2006)

Case #126: Alcatel

Case ID	#126 , level 3
Title	Alcatel
Researcher	Christian van 't Hof
Timing	2006
Geography	Global company, office in Rijswijk the Netherlands
Environment	Office
Technology	Active tags from Wavetrend carried by personnel and placed in lap tops and beamers. Readers are placed at doors and in ceilings and connected with DSmarttech system, based on Windows 2003 server and an SQL database. [1]
Costs	Cost of the RFID system: € …, Implementation costs: € …
Maturity	fully operational
Function	Hands-free access, evacuation management, theft prevention and time registration
Owner	Alcatel provides communications solutions to telecommunication carriers, Internet service providers and enterprises for delivery of voice, data and video applications to their customers or employees. With sales of EURO 13.1 billion and 58,000 employees in 2005, Alcatel operates in more than 130 countries. [4]This story is on the Dutch office in Rijswijk, which has 230 staff members.
Maintainer	Transquest
Users	Alcatel staff
Other actors	Workers Council at Alcatel
Case story	In the beginning of 2005 the Alcatel office in Rijswijk shifted from magnetic card access to active (battery powered) RFID access. All employees received a thick card (100, 50, 5 mm), with a picture on it of themselves, to be carried visibly at all times. An active RFID chip inside the card broadcasts a signal every 1.5 seconds. Readers are placed at all doors and throughout the halls. The system as a whole registers the whereabouts of all the tags in the building in real time. Guest at the office also receive an active tag, of which the identity is linked to the person receiving the guest. Valuable devices such as lap tops and beamers are also tagged with active RFID. [1] This serves several functions: 1. Automating access. On arrival, employees go through three access points: the parking lot (if they come by car), entrance to the building and the staircase or elevator. With active RFIDs, the users don't have to hold their cards near a reader, but just wave it in its direction or not at all. 2. Evacuation management: in the event of an evacuation, facility manager (Hans van der Kooij) rolls out a list of the database to see if there are any persons left in the building and where they may be. 3. Time registration: the database registers the time of entry and exit of all employees. The net time spent in the office is presented in a time registration sheet to the employee, who then justifies hours spent on projects. 4. Preventing theft. The identity of tagged lap tops and beamers is linked to the rightful owner. Once a device leaves the building without its rightful owner, an alarm is set off. The system sends it's coordinates to the camera surveillance system, which is viewed by the receptionist real time. Still, this is what the system is supposed to do. Once the principles have been put into practice, some remarkable things happened. First, the automated access. Although the RFIDs are active, being powered by a battery in order to broadcast their signal, the communication between tag and reader does not always work properly. The reader at the entrance of the parking lot appears to have its moods, presumably depending on the whether. Some readers on one floor appeared to register people moving on another. This was just a matter of adjustment. Still, the exit reader does not always register exit, presumable because several people move through at the same time. Also, office buildings tend to

	have several exits clustered together, causing a single approaching employee opening the elevator, hall door and fire escape at the same time - the latter setting off an alarm. [2] Second, the evacuation management. Every now and then, the Alcatel office holds an evacuation trill. Facility Manager Hans van der Kooij then sets off the alarm and the staff is expected to leave the building. At their first trill with the new system, Van der Kooij came out last, disappointed, holding four tags which were left on the desks. [2,3] Third, time registration. This system may appear as a punch card system but it actually isn't. The simple reason for this is that only less than 25% of staff performs their work only in the office. The rest of them are continuously on the move for their customers. Also some persons live quite distant from the office and are allowed to add some travel time to their working time. The time being registered by the system is therefore merely a helping tool for the employees to fill in their time sheets themselves. Our respondent Jan Vet for example, just came back from a customer in Luxembourg and had to add 14 hours to the sheet. It would otherwise say Jan hadn't been at work at all these days. Also, some flaws occur, especially on checking out of the office. Then the system registers the employee entered, but never left the building, urging employees to maintain all kinds of paper based registries. More fundamentally, the time registration triggered a debate on effort versus effectiveness. Especially the sales representatives claimed they wanted to be accounted for their results and not their time spent. One could be wining and dining with potential customers all the time, while what really matters is getting deals done. This focus on results remains the corporate culture, despite the time registration system. If for example a person turns out to be just three hours in the office on a single day, this does not trigger any response from personnel management. Staff is just trusted for doing their work well. [2,3] During the implementation of the system, the Workers Council got involved as they received questions from staff members. A small number of people argued the system to be a "Big Brother tactic", scanning all their movements through the building. It turned out one specific sails representative triggering this issues. He turned out to have major difficulties with time registration, as described above, which is in fact an issue in its own and not linked to the RFID system. It did however demonstrate how easy the Big Brother scenario is used in this context. The rest of the questions mainly revolved around what would happen with the information registered by the system. For example: "where is the information stored", "who has access to it", "how long are the data retained" or "is it connected to our desktop phones"? Also, some doubted the effectiveness: "what is wrong with the current system" (magnetic cards) or "who don't we develop such a system our selves"? In response Jan Vet and his colleagues checked the implementation with a number of legal advisers and used a checklist of the Dutch privacy office. Reading this checklist, one can recognise the Fair Information Principles. Finally, some persons worried that the radiation of the active RFIDs and readers could cause cancer. [5] All in all, implementing an active RFID system in order to track personnel may appear quite invasive at first hand while in practice it proved to be not so exceptional. Aside from some practical matters, the system was accepted by the staff quite easily. Jan Vet stated one of the reasons may be that, as they work for large telecoms, they are use to high tech, high security environments. [2] Also, the system could be used to evaluate the functioning of staff members on the basis of their movements, but it is not. It remains, above all, a security system. One of the reasons for this may be that the Workers Council was involved in the implementation from the start. Jan Vet, member of the Workers Council, stated: "I consider myself to be a quite anarchic person, but if you describe this system as Big Brother, I think that is a gross statement. You are being followed through your GSM and while you surf the internet. RFID is not much worse than that." [2] Moreover, the system is not used beyond its purpose, e.g. to evaluate personnel productivity based on their movements or whereabouts. One thing he does worry about is what governments will do now RFID is implemented on such a large scale. "Governments should be liable in using these systems. Their hunt on so-called terrorists should not evolve into permanent scrutiny, which I think is disproportional compared to, say, casualties of car crashes." [2] Now the system is fully operational and accepted it is turning into the advantage of the staff: they use the time registration to prove they are overburdened with work. As any telecom, Alcatel cut

	down on personnel during the recent telecom crash. Now business is improving, the workload increases while few new staff is hired. Overwork was claimed to be incidental, but, with the time registration in hand, the Working Council demonstrated is was structural, for some even beyond the boundaries set by labour laws. [2] During our visit at the office, some employees suggested the system could be expanded to enable Private Printing. This involves the printer down the hall being sensitive to the presence of the person giving the print command. This will not only prevent sensitive material being read by others, but will also cut down on the huge pile of prints that are never collected. [3]
ID issue	The system was applied foremost as a security system (evacuation and theft prevention) but soon evolved as a tracking and time registration device. During the implementation phase complaints and worries were expressed by a small number of employees, some claiming it to be a Big Brother system. These matters were addressed by the Workers Council and soon the discomfort faded away. Afterwards, the time registration system was even used to advantage of the staff to show how much overwork they were performing. [2]
Sources	[1] "Handsfree toegangscontrole draagt zorg voor tijdsregistratie en evacuatiemanagement" www.transquest.com [2] Interview with Jan Vet, Technical Project Manager Operations and member of the Workers Council. {3] conversations with Alcatel personnel passing down the hall [4] www.alcatel.nl [5] Alcatel Workers Council questionnaire on the new access system, 31 January 2005

Case #128: Mol Logistics

Case ID	#128 , level 3
Title	Mol Logistics
Researcher	Christian van 't Hof
Timing	2006
Geography	Tilburg, Netherlands
Environment	Office
Technology	Active RFID
Maturity	Pilot / just implemented / fully operational
Function	Access / security / identification
Owner	Mol
Maintainer	TransQuest Tag & Tracing Solutions B.V.
Users	Mol employees, visiting drivers, temporary labour forces
Other actors	
Case story	Mol-Logistics [case 128] is a company specialising in logistics and has considerable experience of using RFID for cargo. The technology is now extended to monitor personnel movements too. Their location in Tilburg is divided into zones by a number of strategically placed RFID readers, both at the truck area as well as the offices. Each truck driver and office staff member carries an active RFID tag which broadcasts a unique signal every 1.5 seconds. The database thus provides a real time image of who is present in which zone, managing the identity of all people inside the premises based on time, place and access levels. First of all, the active RFID tag serves as a key to open the fence, providing access to drivers and as a hands free door opener at the offices. Secondly, it also serves to deny access, for example for visiting drivers who receive active tags too. As long as they remain in the docking area nothing happens. Once the visitor moves into a restricted area, for example the warehouse, an alarm is triggered. Thirdly, at the offices, the tag functions as a punch card, registering time-in and time-out as personnel enter and leave the office. Finally in case of an emergency, security personnel can immediate spot whether there are still people in the danger zone.
ID issue	How do the users and maintainers of the RFID environment define what kind of personal information is known, to what purpose is it used? Is there a controversy?
Sources	Transquest: MOL Logistics Handsfree toegangscontrole draagt zorg voor tijdregistratie en veiligheid (2006)

Case #129: AlpTransit Gotthard AG

Case ID	# 129, level 2
Title	AlpTransit Gotthard AG
Researcher	Christian van 't Hof/Eefje Vromans
Timing	2006
Geography	Italy
Environment	Work
Technology	Active RFID tags
Maturity	fully operational
Function	Security
Owner	Alptransit Gotthard
Maintainer	Acter ag
Users	Workers and material in the tunnel; visitors
Other actors	Techselsta (Lugano, CH), TransQuest Tag & Tracing Solutions B.V
Case story	AlpTransit Gotthard AG is currently building a 57 km long railway tunnel in the Alps. Personnel and material (trains), but also visitors are being monitored by a system of active RFIDs and a series of RFID readers throughout the tunnel. During construction a full map of the situation can be given real time. [2] The main purpose of the RFIDs is to track down the position of every person in the tunnel in case of an incident in order to guide the rescue team [3,4]. The RFID badges of the personnel contain more personal information than the badges of the visitors (from visitors only the name is stored). It is not known if visitors or workers ever refused to carry a RFID chip because of privacy reasons [3]. It is not clear yet if Alptransit also wants to use RFID in the future for travellers through the tunnel. [5]
ID issue	The only purpose of the RFID badges is to track down people in case of an incident. It is not known if workers or visitors ever refused to use the RFID for privacy reasons [3].
Sources	[1] http://www.alptransit.ch/pages/e/ [2] http://www.transquest.nl/nederlands/gebruikers.php [3] Alptransit (+41(0)918212121), contacted on 07september 2006 [4] http://www.acter.ch/products.php?hauptrubrik=500&product=acterrfid (visited on 07 september 2006) [5] Telephone contact with the Alp Transit Visitors Center

Case #130: Apenheul

Case ID	# 130, level 3
Title	Tracking visitors flows through the tagged Monkey Bag
Researcher	Christian van 't Hof
Timing	2006
Geography	The Netherlands
Environment	Leisure
Technology	The system consists of active RFID tags sowed into the visitors bags and 11 reader/buffers defining 10 areas through the park. The readers are stand alone, their data is downloaded weekly. Numbers of visitors per area, time spend en speed of movement through the park are provided in Excel and Acces spreadsheets. Visitors profiles and an overview of the total flow of visitors emerge after analysis.
Costs	Each RFID tag costs €. 25,-, the whole system about € 20.000,-
Maturity	just implemented
Function	Profiling flow of visitors through the park
Owner	Apenheul, a Dutch zoo specialised in monkeys and apes
Maintainer	Wavetrend
Users	Visitors of the park
Other actors	Monkeys and apes
ID issue	This RFID application touches upon the issue on what is personal data and the control costumers should have over data retrieved from their movements. The Monkey Bag RFID has a marketing function: how do visitors move through the park and the flow of people be optimised. The visitors remain unanimous, are not traced real time and do not receive any consequences according to the data they provide. In that sense, the data retrieved cannot be seen as an identity that should be managed from a user perspective. Still, visitors are being traced without informed consent. The tagged bags are provided without informing it's user on the tractability. Moreover, the use of the monkey bag is obligatory. Visitors are given a bag at the entrance with a security argument "Monkeys move freely through the park and will try to steal your goods." Although legitimate in itself, this rule limits free choice of the visitors not to use the bag. A side issue on Identity Management is that the bag is sometimes used by park hosts, to carry food across the park. In order to keep the profiles clean, data on personnel movements need to be erased.
Case story	The Apenheul is a zoo specialised in all kinds of apes and monkeys. An outstanding feature of the park is the opportunity for some kinds of monkeys to move freely through the crowd of visitors. Curious as they are, the monkeys often try to steal or open bags of visitors in the hope to get a free lunch. To prevent this, the park introduced the "Monkey bag", a green bag with an extra clip lock which the monkeys cannot open. This bag is obligatory, which is enforced by the receptionists providing the bag at the entrance of the park and a warning sign. Aside from this security reason for implementing the bag, the department of marketing added a marketing feature to the bag: scanning visitors movements through the park. Currently about 200 of the 3000 bags are tagged. In order to provide a representative sample of visitors, the tagged bags are handed out random, adding to 1 in 15 visitors tracked. A dataset of 90.000 readings provided the data to analyse for visitors flows. If for example an area receives too few visitors, it presumably needs to be made more attractive. If the area receives the most visitors, it's probably a hit. Also, if visitors demonstrate a pattern of "getting lost", e.g. moving back and forth a lot between two area's, the directions need to be changed. Finally the overview of visitors flows can detect congestion spots that need to be relieved. Odd routings are filtered out of the database manually. For example tags that did not pass the first reader, only passed less than five readers or move real fast are presumably personnel carrying the bags. In this way, the system manages identities through differentiating between personnel and visitors.

	According to several park hosts, visitors were informed on the presence of the tag during a pilot phase, but this policy has changed as people then may refused the bags. Marketing manager Smit remarked afterwards there is no reason to inform the visitors on the presence of the tag as it does not gather personal data, only anonymous movements. The Apenheul therefore complies with privacy laws. One of the park hosts, who recollects the bags at the exit, receives questions sometimes from visitors who discover the tag (it's tangible, about 4 to 10 cm and sowed into the inside of the bag). Visitors reacted surprised, but never with much discontent. Real time tracking (more expensive) is currently not necessary for analysing the flow of visitors. Still, the reader at the exit of the park is connected to a visual alarm in order to prevent visitors taking the bag. Each year, about 1 in 3 bags are taken by visitors. In the future all bags will be tagged, so theft will be less likely to occur. Also, once real time scanning will be used, the park will have the opportunity to direct personnel to crowded areas, for example catering. This case clearly enters the grey area on what can be viewed as personal data and to what extend users need to know about information being gathered on their movements. The marketing department of the Apenheul balanced between informed consent and spoiling the data gathering. If they do not inform their visitors they will run the risk of public controversy once the story gets out into the open. But if they do, some visitors may refuse using the Monkey Bag, preventing the net sample of visitors profiles less representative.
Sources	We discovered this case through the website of the provider Wavetrend. We then contacted the Apenheul and visited the park at the 3rd of August 2006 for observations and eight short interviews with park hosts. Finally we held a telephone interview with marketing manager Bert Smit 22 august 2006. De Apenheul Park Berg en Bos J.C. Wilslaan 21-31 7313 HK Apeldoorn Phone: 003155-3575757 E-mail office@apenheul.nl

Case #131: Exxon Mobile Speedpass

Case ID	#131 , level 1
Title	ExxonMobile Speedpass
Researcher	Christian van 't Hof
Timing	1997-2006
Geography	US, Canada, Singapore, Japan
Environment	traffic and retail
Technology	The Speedpass consists of a 134kHz RFID chip (Texas Instruments) in a small black plastic barrel of about 2 cm which can be carried on a keychain. Readers are placed at the gas dispenser and at the cashier. Communication between reader and tag is secured through a challenge response protocol, which works as follows. When the readers sends out its signal, a random number is given. The chip performs a mathematical operation on the number, using its own secret code and sends back the result together with its serial number. The readers sends this information through satalite communication to the central database in Houston, which have lists of all authorised Speedpass owners, perform the same calculation as the tag and compare the result. If the numbers match, the purchase is made through the customers credit card number. This proves takes about 3 seconds. [4]
Costs	Cost of the RFID system: $ 60.000,- for each location. [4] Customers can order and use the tag free of charge.
Maturity	fully operational
Function	payment
Owner	The Speedpass system was developed by ExxonMobil.
Maintainer	ExxonMobile. The radio frequency technology is provided by Texas Instruments and integrated into the fuel dispensers by the Wayne Division of Dresser Industries.[3]
Users	Customers at the gas station
Other actors	Trials at McDonalds and Stop & Shop.
Case story	Speedpass is a RFID pay system at ExxonMobile gas stations. The pass consists of a small black plastic barrel of about 2 cm which can be carried on a keychain. Readers are placed at the pump and cassier. The RFID chip in the barrel carries a unique code which is connected to the holders credit card account. It was first introduced at Mobil-branded service stations in 1997 as an easy and fast way to pay at the pump. Soon, the Speedpass system was extended to Mobile's convenience stores. After the merger with Exxon, the pass was employed at the Exxon stations too. By 2003, there were over 5 million activated Speedpasses, accounting for 10% of sales at the pump. In 2005, Speedpass is deployed at 8,600 locations throughout the US. [4] During it's implementation phase, several trial were held to extend the reach of the Speedpass system. In 2001, ExxonMobile started trials at 450 McDonalds in the Chicago area and in 2003 with Stop & Shop supermarkets to see whether the pay system could be extended to fast food and groceries. Speedpass was origionally employes just for paying gas, but according to Joe Giordano, vice president of systems en product development at Speedpass their customers expressed the need to use it at other "around-the-town, convenience oriented-type purchases". Still, for some reason or another, we were unable to find many accounts of this use today. More than 6 million Speedpass devices have been issued in the U.S. Exxon- and Mobil-branded service stations and convenience stores in the U.S. There are more than 8,800 locationsExxon- and Mobil-branded service stations and convenience stores in the U.S. in the U.S. that accept Speedpass. Research shows that more than 90 percent of Speedpass users report they are highly satisfied. Nearly 2 million Speedpass devices have been issued in Canada, Singapore and Japan for use at more than 1,600 retail locations in those countries. [3] Each device has a unique identification and security code that is transmitted to the reader when you make a purchase. The purchase is automatically charged to the payment method linked to the Speedpass device. The customer's credit or check card number (or checking account number) and personal information are never

	stored in the Speedpass device and remain outside the Speedpass signal system, maintaining the confidentiality of that information. [3] First the developers of Speedpass tried the same technology as in toll roads, i.e. active high frequency RFID which can be read while driving at high speed. This did not work because of the large read area of active RFID, making it impossible to distinguish who was using which dispenser. Addionally, the costs of the active RFID were much higher. Moreover, the passive RFID gives the customer control over the act of paying: they have to wave it in front of the reader, as with an active RFID they could be read anytime without noticing.
ID Issue	The Speedpass is not just used to pay, but also has a marketing purpose. This is clearly stated in the "Privacy Policy" and "Terms of use", which users are assumed to have read and agreed upon when they subscribe to the pass. For example: "Speedpass and its affiliates may disclose any of the information that we collect to affiliates and non-affiliated third parties as described below. We may disclose the information whether you are a current customer or former customer." Among parties mentioned are security services, mortgage banking, direct marketing organisations and "any bidder for all or part of the Speedpass business". In practice this will mean the identity "person paying at the pump", through travel- and consuming profile, could evolve into "potential valuable customer for a motel, mortgage or groceries" or "a potial link to a criminal network". Once a customer uses the Speedpass for the first time, this act is defined as opting in on this policy. The policy also offers an opt out, but if the information is already passed onto another organisation, ExxonMobile does not have control or responsibility over it.Additionally, users can maintain their user profile on line, e.g. view their transactions and receive receipts on line. An IDM issue arising here is one family member tracing another, for example a suspicious spouse. Another IDM issue is when the Speedpass is not used by it's rightful owner. Tags are lost or stolen. Moreover, they can be copied. Researchers at the Johns Hopkins University and RSA Laboratories for example succeeded in reading a Speedpass, cracking the code and reproduce another tag. In order to prevent misuse "Speedpass monitors purchase patterns on Devices, and looks for unusual behaviour that may signal unauthorized use." [2] So, comparable to how credit companies operate, Speedpass analyses transactions in real time for awkward profiles. If for example an unusual large purchase is made, or purchases occur at awkward locations, the transactions may be blocked and checked at the rightful owner of the pass. Still, while these profiling analyses run real time, one could wonder whether these profiles are only used to prevent fraud. Still, although the Speedpass system could in principle facilitate all sorts of direct marketing efforts, tracking of people or fraudes, accounts on it's current use indicate otherwise. On on line discussion groups for example, many people express their fear on Big Brother scenario's, but none claim to actually encountered privacy invading actions. Most of the discussion treats mainly evolve around practical matters: on how the system works, if it really saves time or at which gas stations it can be used.
Sources	[1] Speedpass Privacy Policy: https://www.speedpass.com/forms/frmDynPrin.aspx?pId=2 (28 august 2006) [2] Speedpass Terms of use: https://www.speedpass.com/forms/frmDynPrin.aspx?pId=23 (28 august 2006) [3] Speedspass Factsheet: http://www2.exxonmobil.com/corporate/files/corporate/speedpass_fact_sheet.pdf#search=%22speedpass_fact_sheet%22 (28 august 2006) [4] Garfinkel, S. "RFID Payments at ExxonMobil" In: Garfinkel, S. & Rosenberg, B. (ed.) RFID. Applications, Security, and Privacy. [5] For example: alt.tv.pol-incorrect, misc.activism.progressive or alt.culture.ny-upstate [6] For example: misc.transport.road [7] Biba, E. (2005) "Does your Car Key pose a Security Risk?"In PC World 14 February

Case #133: Medixine

Case ID	# 133, level 1
Title	Medixine RFID Communication Board
Researcher	Jessica
Timing	End of 2005
Geography	Finland (Imatra)
Setting	Healthcare
Environment	Homecare
Technology	RFID communication board: the board can be fitted with up to 6 NFC-RFID tags. NFC enabled mobile phones: mobile phone equipped with RFID reader Medication Management Server Application
Maturity	Pilot
Function	Informative for users (medication compliance)
Owner	Medixine [66]
Maintainer	Medixine
Users	- Patients enrolled in the trial - Medical staff enrolled in the trial - Caretakers and family of patients enrolled in the trial
Other actors	- Nokia > provider of cell phones [67] - Alzheimer Society of Finland > financial support [68] - Pfizer > production of Alzheimer drugs [69] - Elisa > provider of wireless network [70]
Case story	The system should make sure that Alzheimer patients take their drugs. Each tag on the communication board can be assigned to a specific situation and is represented by a symbol. In the trial three situations are tested. One is the confirmation that medication has been taken, another is a request for someone to call for a chat and the third requests an immediate call in response to an emergency. The patient activates a situation by touching the symbol with the NFC-enabled cell phone. This message is then broadcasted over a network and compared to the patient's record, if necessary other people are informed [71, 71]. Trial were patients and items that are part of their treatment are tagged, seem to be turning up all around Europe, for instance in the Ospedale Maggiore in Bologna, Italy and in the Klinikum Saarbrücken in Saarbrücken, Germany [7,8]. When a patient arrives at the hospital he or she receives an RFID bracelet. This bracelet makes it possible for hospital staff to identify the patient and to access medical records quickly and apply treatment with more accuracy. Also, blood bags are tagged by the hospital. All patient records and blood supply information are held on a secured database, which can be accessed by medical personnel through a PDA. Medical records are constantly updated, based on the reading of the PDA's. In Italy, there is a extra security measurement: only after a fingerprint-based biometric authentication is completed a person can read the identifications of the patient and the blood unit being used in any transfusion. If the unique identifiers on the patient and the blood unit are a match, a wireless electronic seal on the blood unit is released, permitting the transfusion to occur. A similar trial is also being executed at the Amsterdam Medical Centre in Amsterdam, The Netherlands [9]. Besides matching and error prevention of blood transfusion materials, individuals working in the operation rooms (OR) are identified and localised, as well as OR-materials.
ID issue	In this case, strict supervision by a medical team is necessary because patients are not capable of taking care of themselves. The technology brings this supervision as far as in people's own houses. On the other hand, without the system the patients might not even be living in their own houses anymore.
Sources	66.http://www.medixine.com (visited 5 September 2006) 67.http://www.nokia.com (visited 5 September 2006) 68.http://www.alzheimer.fi (visited 5 September 2006) 69.http://www.pfizer.com (visited 5 September 2006)

70.http://www.elisa.com (visited 5 September 2006)
71. Collins, J., 'Medixine Tests System for Alzheimer's.' In: RFID Journal, 27 September 2005 (http://www.rfidjournal.com/article/articleview/1892/1/1/, visited 5 September 2006)
72. 'RFID Technology for Blood tracking: a new application finds Ospedale Maggiore.' In: RFID Gazette, 20 June 2006
73. 'Saarbruecken Clinic adds stocks of stored blood to its RFID pilot project.' Siemens Business Services Press Release, Munich, 20 February 2006
74. 'Zorgsector start proef met RFID.' (http://www.rfidnederland.nl/Default2.aspx?tabid=264, visited 13 september 2006)